Redes de Computadores

Prof. Me. Wesley Viana

- Unidade de Ensino: 03
- Competência da Unidade: Redes de Computadores
- Resumo: Introdução a Redes de Computadores
- Palavras-chave: Redes de Computadores; Protocolos; Teleprocessamento; Aplicações; Modelo OSI.
- Título da Teleaula: Arquitetura e tecnologias de redes;
- Teleaula nº: 03

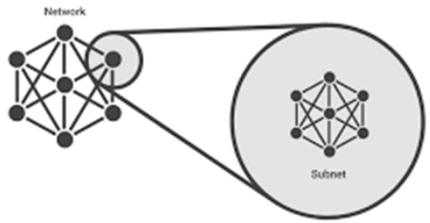
Contextualização

- Redes e sub-redes;
- Ethernet;
- IPv6.

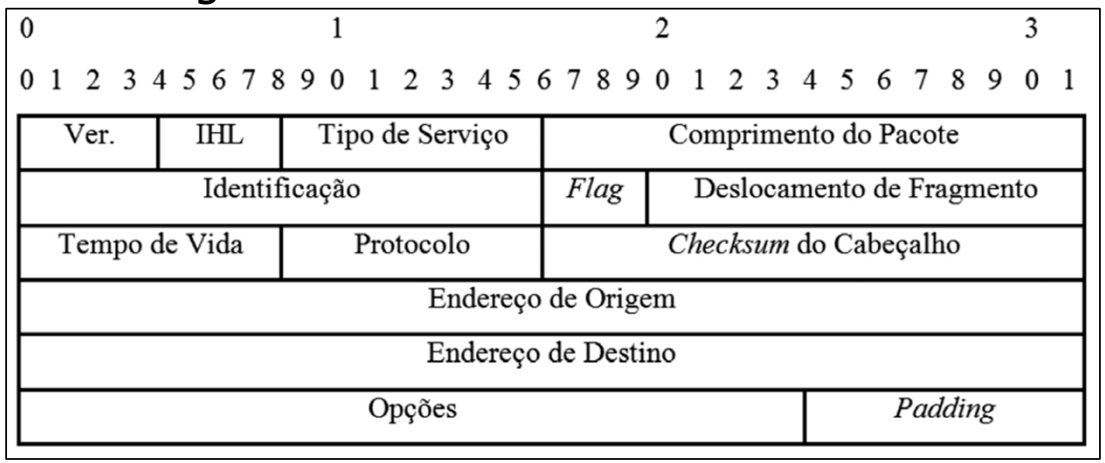
Redes e sub-redes

Redes e sub-redes

Segundo Kurose (2006), o Internet Protocol, ou simplesmente IP, é o endereço lógico feito para que um dispositivo possa se comunicar com qualquer outro dispositivo, independentemente de sua localização geográfica.



Conforme determina a RFC 791 (para a versão 4), o IP possui 32 bits, sendo possível produzir 2^{32}= 4,3 bilhões de endereços. O protocolo está definido na camada de rede, sendo o seu pacote denominado datagrama.



Redes e sub-redes

Versão: campo que traz a versão do protocolo IP (4 ou 6).

IHL: determina o tamanho do cabeçalho.

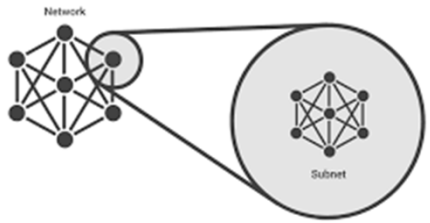
Tipo de serviço: determina a prioridade do pacote.

Comprimento do pacote: fornece o tamanho total do pacote, incluindo o cabeçalho e os dados.

Identificação: identifica o fragmento do pacote IP original.

Flag: é dividido em Flag mais Fragmentos (MF), usado para o deslocamento dos datagramas e, posteriormente, a sua reconstrução, e em Flag não Fragmentar (DF), que indica que a fragmentação do pacote não é autorizada.

Deslocamento de fragmento: responsável por identificar a ordem dos pacotes no processo de remontagem.



Redes e sub-redes

Tempo de vida: identificado como TLL (time to live), indica o "tempo de vida" que o pacote possui a cada salto pelos nós.

Protocolo: responsável por repassar os dados para os protocolos corretos que estão nas camadas superiores.

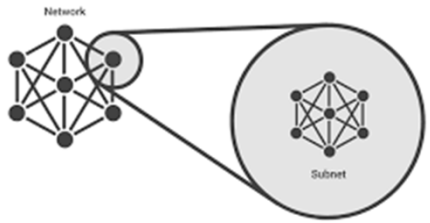
Checksum do cabeçalho: responsável por informar os erros no cabeçalho.

Endereço de origem: identifica o endereço do remetente.

Endereço de destino: identifica o endereço do receptor.

Opções: implementações opcionais.

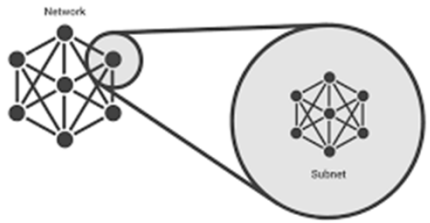
Padding: preenchimento.



Redes e sub-redes

Para a compreensão do formato do endereçamento IP, faremos uma analogia com os números utilizados em telefonia fixa.

Seguindo essa lógica, a notação de um endereço IP é separada por ponto, fazendo com que uma parte identifique a rede e a outra, o dispositivo (host).



Por exemplo:

172.16.30.110

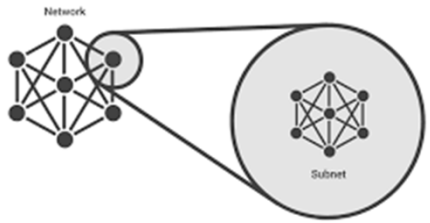
172.16 → identifica à qual rede o dispositivo pertence.

30.110 → determina o endereço do dispositivo.

Segundo Kurose (2006), os endereçamentos utilizados nas redes foram divididos em classes para utilização de acordo com o número de dispositivos da rede, conforme é possível observar.

Redes e sub-redes

	8 bits	8 bits	8 bits	8 bits	Intervalo
Classe A	NETI	HOST	HOST	HOST	0 – 127
Classe B	NET	NET	HOST	HOST	128 – 191
Classe C	NET	NET	NET	HOST	192 – 223
Classe D	Classe reservada para endereços de multicast				
Classe E	Classe reservada para pesquisa				



Exemplos de cada uma das classes:

Classe A: 10.0.0.50, em que 10 é o endereço de rede e 0.0.50 é o endereço de host;

Classe B: 172.16.31.10, em que 172.16 é o endereço de rede e 31.10 é o endereço de host;

Classe C: 192.168.0.20, em que 192.168.0 é o endereço de rede e .20 é o endereço de host.

Redes e sub-redes

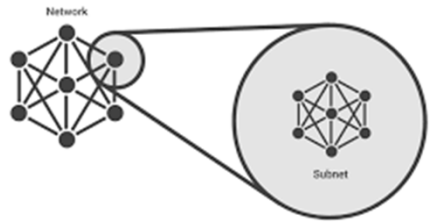
Além da divisão por classes, a utilização deve obedecer:

IP para rede privada: números de IP reservados para utilização dentro das LANs

Classe A: 10.0.0.0 a 10.255.255.255

Classe B: 172.16.0.0 a 172.31.255.255

Classe C: 192.168.0.0 a 192.168.255.255



IP para rede pública: faixas de números de IP utilizados para dispositivos acessíveis pela internet. Por exemplo, os servidores como o 201.55.233.117 (endereço do site google.com.br).

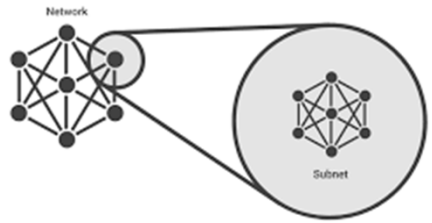
Configurar os IPs dos dispositivos de uma rede, são necessárias algumas configurações.

```
Endereço IPv4. . . . . . . . . . . . . . : 192.168.0.101
Máscara de Sub-rede . . . . . . . . . . . : 255.255.255.0
Gateway Padrão. . . . . . . . . . . . . . : 192.168.0.1
```

Redes e sub-redes

Gateway saída das mensagens na rede interna. Normalmente é o IP do equipamento (roteador ou switch) na borda da rede interna.

Máscara de sub-rede é a técnica utilizada para definir qual porção do número IP é designada para identificar o host e a rede (network).



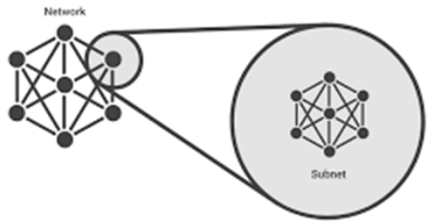
Segundo Filippetti (2008), a máscara de rede possui 32 bits, possuindo padrão para as classes A, B e C.

Classe	Formato	Máscara padrão
A	Rede.Hbst.Host.Host	255.0.0.0
B	Rede.Rede.Host.Host	255.255.0.0
C	Rede.Rede.Rede.Host	255.255.255.0

Redes e sub-redes

Para isso, lembre-se de que a contagem dos números IP vai de 0 a 255, podendo se representar pelos valores: 128, 64, 32, 16, 8, 4, 2, e 1. Se efetuarmos a soma desses valores, teremos 255, ou seja, é possível representar qualquer endereço de rede binariamente, no intervalo de 0 a 255.

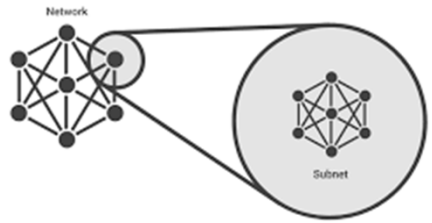
Segundo Tanenbaum (1997), também conhecida como subnet, que podem ser isoladas das demais ou não.



Redes e sub-redes

Isso permite que o administrador dentro de uma faixa de IP possa ter:

Redução do tráfego de rede, pois os nodos dentro das subredes fazem domínio de broadcast, mensagens enviadas para todos os nodos da rede.

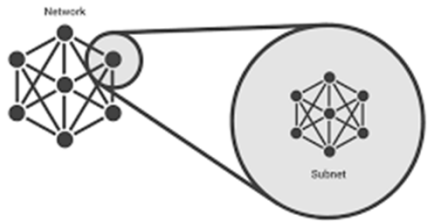


Simplificação no gerenciamento da rede, pois facilita-se a identificação de falhas pelo mapeamento do endereço da sub-rede.

Controle dos recursos da rede, pois possibilita-se “enxergar” uma grande rede, como diversas LANs isoladas.

Redes e sub-redes

Para calcular as sub-redes, vamos tomar de exemplo uma rede de classe C, em que a faixa de IP utilizada deve ser 192.168.0.0; e a máscara padrão, 255.255.255.0, sendo desejado fazer quatro subredes. Para isso, Filippetti (2008) define que:



1º passo: faça a conversão da máscara de rede para binário

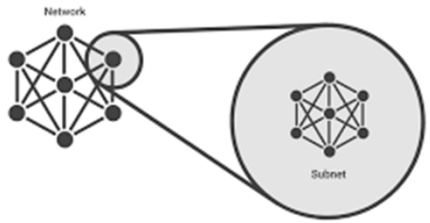
2º passo: efetue o cálculo da quantidade de hosts possível em cada uma das sub-redes

Lembre-se de que para converter os octetos, são utilizados: 128, 64, 32, 16, 8, 4, 2, 1; portanto, se, para determinar o número de redes, foram emprestados 2 bits, então sobraram 6 bits para determinar o número de hosts.

Redes e sub-redes

3º passo: construa a tabela de sub-redes:

Rede	1º IP Válido	Ultimo IP Válido	Broadcast
192.168.0.0	192.168.0.1	192.168.0.62	192.168.0.63
192.168.0.64	192.168.0.65	192.168.0.126	192.168.0.127
192.168.0.128	192.168.0.129	192.168.0.190	192.168.0.191
192.168.0.192	192.168.0.193	192.168.0.254	192.168.0.255



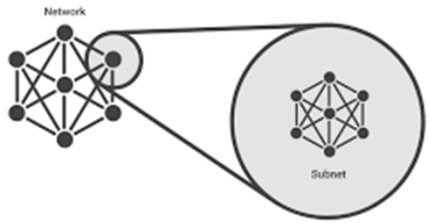
4º passo: determinar a nova máscara de rede:

Ou seja, são representados o endereço IP 192.168.0.1 utilizado para identificar um dispositivo e a sua respectiva máscara de rede 255.255.255.192. Para utilizar essa técnica para desenvolvimento de sub-redes nas classes A e B, deve-se seguir o mesmo conceito apresentado para a classe C.

Redes e sub-redes

Endereço de broadcast

Commer (2007) indica a difusão de um pacote para todos os dispositivos da rede (se o contexto for de uma sub-rede, então somente aos dispositivos desta). Ao receber a mensagem, o dispositivo deve “ler” o pacote e verificar se lhe pertence.

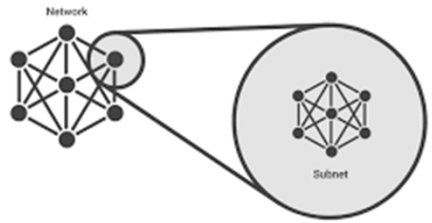


Se pertencer a ele, a mensagem é respondida, caso contrário o pacote é descartado. Veja um exemplo: ao ligarmos um computador em uma rede, este emite uma mensagem de broadcast solicitando um endereço IP ao servidor DHCP.

Redes e sub-redes

Endereço de loopback (127.0.0.1)

Trata-se de um endereço reservado para teste de comunicação nos processos ocorridos na interface de rede do próprio dispositivo.

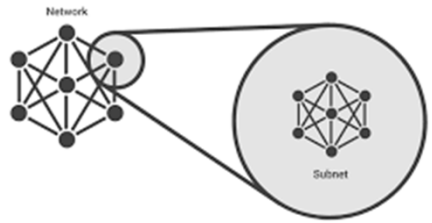



```
C:\Users\Prof. Serginho Nunes>ping 127.0.0.1

Disparando 127.0.0.1 com 32 bytes de dados:
Resposta de 127.0.0.1: bytes=32 tempo<1ms TTL=128
Resposta de 127.0.0.1: bytes=32 tempo<1ms TTL=128
Resposta de 127.0.0.1: bytes=32 tempo<1ms TTL=128
Resposta de 127.0.0.1: bytes=32 tempo<1ms TTL=128

Estatísticas do Ping para 127.0.0.1:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
             perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 0ms, Máximo = 0ms, Média = 0ms
```

É possível confirmar o funcionamento da interface de rede e o protocolo TCP/IP quando são enviados quatro pacotes com todos recebidos, dentro do tempo (1 ms).

Redes e sub-redes

Tanenbaum (1997) define que o roteamento é a técnica utilizada para encaminhar as mensagens através das redes. Os processos envolvidos devem:



- Determinar os caminhos possíveis da origem até o destino.
- Selecionar o melhor caminho.
- Identificar se o pacote pertence a uma sub-rede e garantir que ele alcance o seu destino.

Dessa forma, equipamentos como os roteadores (os switches gerenciáveis também) podem consultar a sua tabela de roteamento e, por meio do endereçamento disponível no cabeçalho TCP/IP, efetuar o encaminhamento correto das mensagens.

Ethernet

Ethernet

Ethernet

Tecnologias utilizadas nas redes Ethernet, os domínios de colisão e broadcast. Segundo Tanenbaum (1997), pode se definir Ethernet como um padrão utilizado em transmissões em redes locais (Norma IEEE 802.3). As normas IEEE 802 possuem subgrupos.

Subgrupo	Definição
IEEE 802.1	Gerência de rede
IEEE 802.2	*Logical link control*
IEEE 802.3	Ethernet
IEEE 802.5	*Token ring*
IEEE 802.6	Redes metropolitanas
IEEE 802.7	Rede metropolitana
IEEE 802.8	Fibra óptica
IEEE 802.10	Segurança em rede local
IEEE 802.11	Rede sem fio (Wireless)
IEEE 802.15	Rede PAN (bluetooth)
IEEE 802.16	Rede Wi-Max

Ethernet

As características técnicas e demais assuntos relacionados às redes locais (Ethernet).

• Conexão dos dispositivos: devem estar conectados em uma mesma linha de comunicação.

• Meios de ligação: devem ser constituídas por cabos cilíndricos.

Diferentes tipos de cabeamentos utilizados nas redes IEEE 802.3:

Ethernet

Sigla	Característica	Cabo	Conector	Débito	Distância
10Base2	Ethernet fina	Cabo coaxial (50 Ohms) de diâmetro fino	BNC	10 Mb/s	185 m
10Base5	Ethernet espessa	Cabo coaxial de diâmetro espesso	BNC	10Mb/s	500 m
10Base-T	Ethernet padrão	Par trançado (categoria 3)	RJ-45	10 Mb/s	100 m
100Base-TX	Ethernet rápida	Duplo par trançado (categoria 5)	RJ-45	100 Mb/s	100 m
CAT6	Ethernet Gigabit	Duplo par trançado (categoria 6)	RJ-45	1000 Mbit/s	550 m
CAT6a	Ethernet de 10 Gigabits	Duplo par trançado (categoria 6)	RJ-45	10 Gbit/s	550 m
100Base-FX	Ethernet rápida	Fibra óptica multimodo (tipo 62.5/125)	****	100 Mb/s	2 km
1000Base-T	Ethernet Gigabit	Duplo par trançado (categoria 5)	RJ-45	1000 Mb/s	100 m

Ethernet

1000Base-LX	Ethernet Gigabit	Fibra óptica monomodo ou multímodo	****	1000 Mb/s	550 m
1000Base-SX	Ethernet Gigabit	Fibra ótica multímodo	****	1000 Mbit/s	550 m
10GBase-SR	Ethernet de 10 Gigabits	Fibra ótica multímodo	****	10 Gbit/s	500 m
10GBase-LX4	Ethernet de 10 Gigabits	Fibra ótica multímodo	****	10 Gbit/s	500 m

Nas transmissões em que é possível alcançar velocidades de 1 Gbps, é utilizado cabeamento do tipo CAT6. Por sua vez, em transmissões com velocidades com até 10 Gbps, utiliza-se o CAT6a.

Segundo Filippetti (2008), o tipo de tecnologia aplicada ao cabeamento dita a velocidade que cada um deles pode atingir, sendo estas as mais utilizadas nas aplicações IEEE 802.3: Fast Ethernet (Ethernet rápida), Ethernet Gigabit, Ethernet 10 Gigabit.

Ethernet

Métodos de transmissão Ethernet

Tanenbaum (1997) aponta que as comunicações desse tipo de rede são efetuadas pelo protocolo CSMA/CD (carrier sense multiple access with collision detection), que permite que qualquer dispositivo da rede possa efetuar uma transmissão sem

hierarquizar quem tem prioridade.

CSMA (carrier sense multiple access – acesso múltiplo com detecção de portadora): trata-se de um protocolo que faz a transmissão com base na detecção da existência de uma transmissão.

Ethernet

É possível utilizar três algoritmos:

CSMA não persistente: se o meio de transmissão estiver ocupado, o dispositivo espera um tempo aleatório e tenta retransmitir até conseguir.

CSMA 1 persistente: o dispositivo "escuta" a rede até que o meio fique livre e, então, procede com a transmissão.

CSMA p-persistente: o algoritmo calcula a probabilidade de colisão e, quando livre e com baixa ou nenhuma possibilidade de colisão, procede com a transmissão.

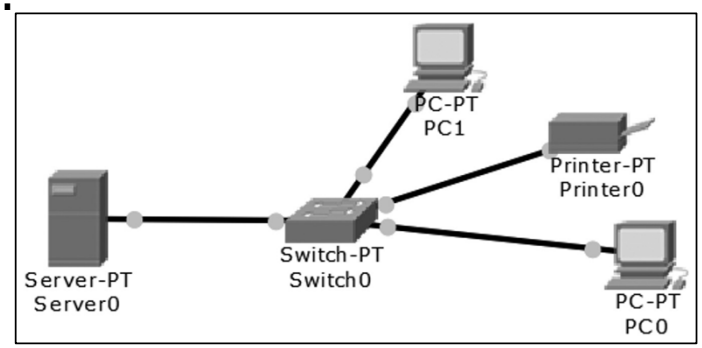
CD (coilision detection – detecção de colisão): o mecanismo CD faz com que os nodos existentes na rede "escutem" a rede e possam detectar colisões (técnica conhecida como LTW – listen while talk – escuta enquanto fala). Quando é detectada uma colisão, o nodo emite um pacote alertando todos os dispositivos.

Ethernet

Tais características encontradas no protocolo CSMA/CD fazem com que tenhamos uma Ethernet comutada. Esse tipo de tecnologia é mais recente, o que permitiu uma evolução nas redes do tipo IEEE 802.3.

Ethernet comutada

Segundo Filippetti (2008), essa tecnologia é constituída em cima de uma topologia estrela, estruturada como nodo central um switch (comutador).



Ethernet

Na comutação, os nodos verificam a porta a que o dispositivo receptor está conectado. Tais técnicas evitam colisões e permitem velocidades de transmissões do tipo 10/100/100 megabits/s no modo full-duplex.

Tanenbaum (1977) destaca que os dois tipos de ocorrências de colisões nas redes Ethernet são:

Domínio de colisão: No domínio de colisão, os pacotes têm a possibilidade de efetuar a colisão uns com os outros. Essa ocorrência é um dos fatores principais da degradação dos serviços; se o equipamento que realiza o domínio de colisão for cascateado, a rede pode sofrer maiores consequências.

Domínio de broadcast: No domínio de broadcast, determina-se o limite a que o pacote pode chegar, ou seja, um dispositivo em uma rede local é capaz de efetuar a comunicação com outro sem que seja utilizado um roteador.

Ethernet

Observe o comportamento dos equipamentos nesse contexto:

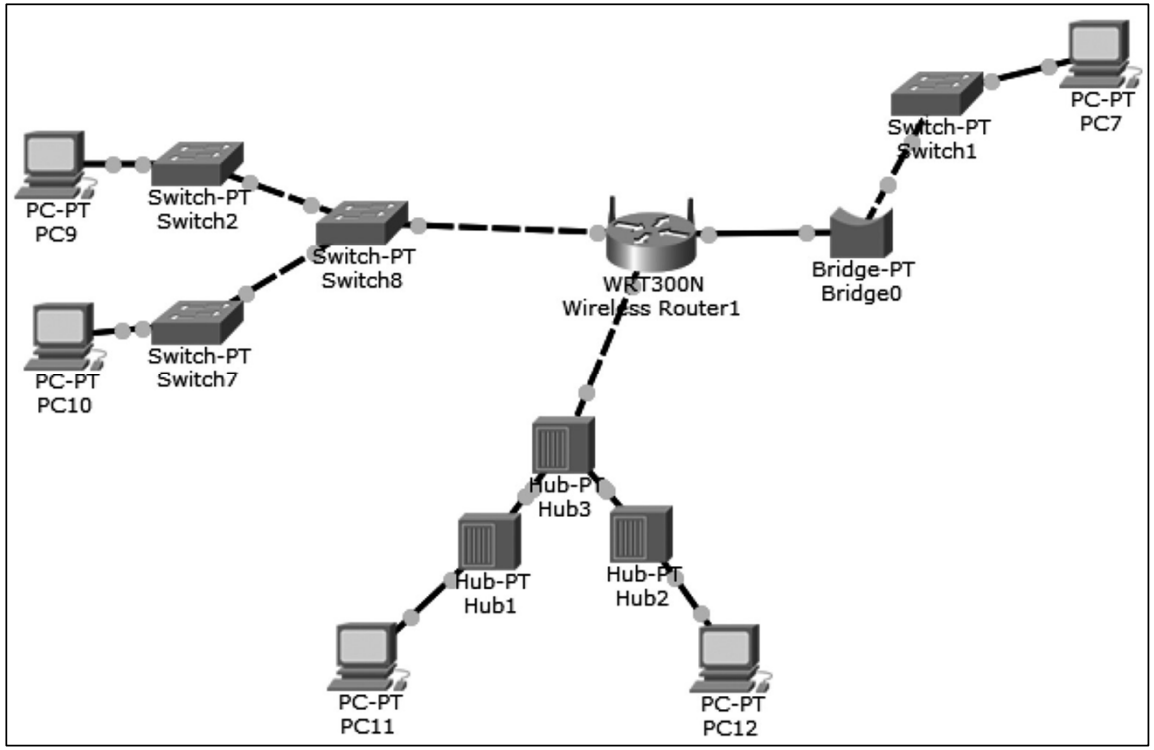
HUB: como são equipamentos que repetem as mensagens para todas as portas, formam um único domínio de colisão e broadcast.

Roteador: são dispositivos concebidos na camada 3 do protocolo TCP/IP – por padrão quebram o domínio de broadcast.

Switch: este equipamento é capaz de formar um domínio de colisão em cada uma de suas portas, em um único domínio de broadcast.

Bridge: este equipamento pode separar domínios de colisão. Como os switchs, formam um único domínio de broadcast.

Ethernet


PC-PT
PC9
Switch-PT
Switch2
Switch-PT
Switch8
WRT300N
Wireless Router1
Bridge-PT
Bridge0
Switch-PT
Switch1
PC-PT
PC7
PC-PT
PC10
Switch-PT
Switch7
Hub-PT
Hub3
Hub-PT
Hub1
Hub-PT
Hub2
PC-PT
PC11
PC-PT
PC12

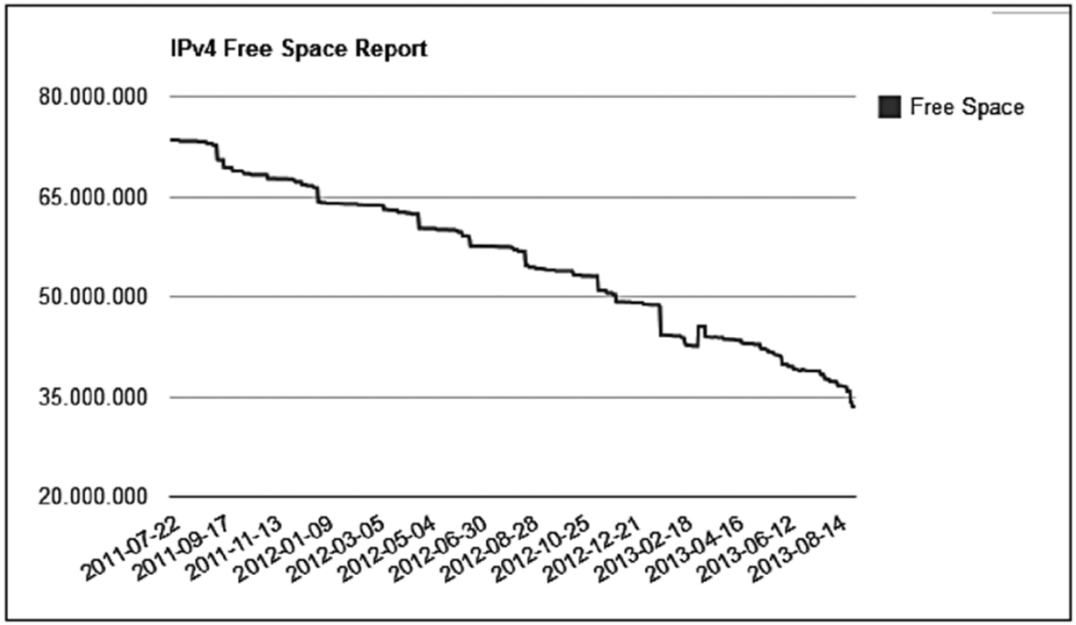

INTERNET

IPv6

IPv6

A LACNIC (Latin American and Caribbean Internet Addresses Registry) é um órgão responsável pelos registros de endereços de internet na América e Caribe.

A LACNIC foi a responsável por efetuar o monitoramento do esgotamento do IPv4.



IPv6

Inicialmente o IPv6 surge no cenário de redes de computadores para suprir as necessidades do IPv4. Segundo Tanenbaum (1997), o novo protocolo deve:

1. Resolver a escassez de endereços.
2. Simplificar o cabeçalho, facilitando o processamento dos pacotes e o aumento da velocidade do envio/recebimento.
3. Tornar opcionais os campos obrigatórios do cabeçalho, facilitando, assim, o roteamento dos pacotes.
4. Garantir a segurança das transmissões, tornando o IPsec obrigatório.

IPv6

Suas características foram definidas por meio das RFCs.

RFC 2460: especificações do IPv6 (12/1998).

RFC 2461: especificações de descoberta de vizinhos IPv6 (neighbor discovery IPv6).

RFC 4291: definição da estrutura do IPv6 (01/2006).

RFC 4443: especificações do ICMPv6 (internet control message protocol).

As especificações desenvolvidas pelos engenheiros da IETF para o IPv6 fizeram com que fosse estruturado o cabeçalho

Versão	Classe de Tráfego	Identificação de Fluxo	
Tamanho dos Dados		Próximo Cabeçalho	Limite de Saltos
Endereço IP de Origem			
Endereço IP de Destino			

IPv6

Versão: indica a versão do protocolo IP utilizada.

Classe de tráfego: indica qual é o nível de prioridade.

Identificação de fluxo: faz o controle de fluxo de informação.

Tamanho dos dados: calcula o tamanho total do datagrama.

Próximo cabeçalho: informa a presença de opções [chama-se de cabeçalhos de extensão].

Limite de saltos: indica número máximo de nós que o pacote

pode atravessar.

Endereço IP origem: define o endereço do remetente.

Endereço IP destino: indica o endereço do destinatário

IPv6

O endereçamento do protocolo IPv6 possui 128 bits (lembre-se de que o IPv4 possui apenas 32 bits), o que possibilita 2128 endereços possíveis, ou ainda 340 undecilhões. O seu formato é dividido em oito grupos com quatro dígitos hexadecimais, conforme pode ser observado: 8000:0000:0010:0000:0123:4567:89AB:CDEF (no IPv4 é dividido em quatro grupos com 8 bits cada, ex.: 192.168.0.100).

Versão / Itens	IPv4	IPv6
Quantidade de endereços	2^{32}	2^{128}
Quantidade de campos	14	8
MTU mínimo	576 bytes	1.280 bytes
Representação do endereço	4 Grupos com 8 bits	8 Grupos com 16 bits
Tamanho do endereço (bits)	32	128
Roteamento	Tabela de roteamento grande	Efetuado pelo cabeçalho de extensão
Segurança	IPSeg facultativo	IPSeg obrigatório
Qualidade de serviço (QoS)	Sem garantia	Através dos campos, classe de tráfego e identificação de Fluxo
Cabeçalho	Uso do checksum	Mais simplificado

IPv6

Tanenbaum (1997) define que, nesse longo período de transição, os administradores de redes e os provedores de internet preveem que possam ocorrer alguns impactos nas redes, como descrito a seguir:

Gerenciamento de falhas: os administradores devem efetuar um plano de contingência para que as redes continuem operando com o IPv4 e IPv6.

Gerenciamento de contabilização: deve-se recalcular os limites de utilização dos recursos, pois com os dois protocolos em operação o consumo muda em relação as redes somente com IPv4.

IPv6

Gerenciamento de configuração: para permitir que os dois protocolos possam conviver nas redes, são necessárias diversas configurações.

Gerenciamento de desempenho: com a mudança de cenário (redes com os dois protocolos operando), o desempenho da rede necessita de adaptações para garantia do acordo de nível de serviço (SLA – service level agreement).

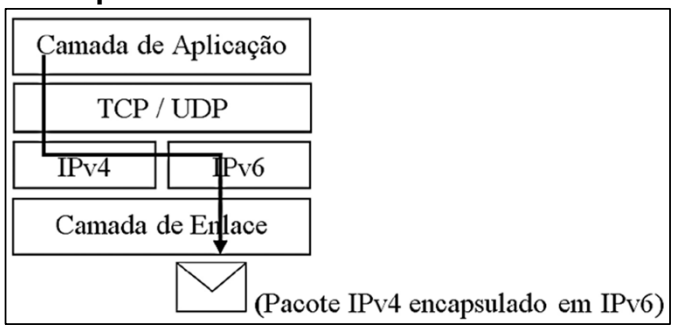
Gerenciamento de segurança: o administrador deve optar por alguma técnica que garanta a interoperabilidade sem gerar riscos à segurança da rede e/ou de usuários.

IPv6

Para resolver esse problema, a IETF formou grupo de trabalho denominado IPv6 Operations para que fossem desenvolvidas algumas normas e diretrizes para redes IPv4/IPv6. Com isso, o mecanismo de pilha dupla foi normatizado na RFC 1933.

Pilha dupla

Segundo Tanenbaum (1997), os dispositivos que têm a pilha dupla ativada terão dois endereços relacionados à sua interface de rede, um IPv4 e o outro IPv6. Para que os datagramas possam "atravessar" a pilha dupla.



IPv6

As mensagens provenientes da camada de aplicação utilizam o encapsulamento na pilha dupla para que sejam enviadas à camada de enlace, que, por sua vez, as conduz à camada física para que, então, sejam enviadas ao meio disponível (cabeado ou sem fio). Nesse sentido, existem duas possibilidades:

1. A mensagem está no formato IPv4 e é encapsulada com IPv6.
2. A mensagem está no formato IPv6 e é encapsulada com IPv4.

Com isso, é necessário que os dispositivos, como computador, servidor, câmera IP, impressoras IP e smartphone estejam com a pilha dupla habilitada.

IPv6

A maioria das versões dos sistemas operacionais atualmente (Windows, Linux e MAC) possui suporte a pilha dupla.

```
Sufixo DNS específico de conexão. . . . . :
Endereço IPv6 de link local . . . . . : fe80::2d91:a36e:e649:cff8%11
Endereço IPv4. . . . . . . . . . . . . : 192.168.0.103
Máscara de Sub-rede . . . . . . . . . . : 255.255.255.0
Gateway Padrão. . . . . . . . . . . . . : 192.168.0.1
```

Outra técnica utilizada para permitir a comunicação entre os dispositivos em redes operando com as duas versões do protocolo é empregar o mecanismo de tradução de endereços.

IPv6

Network Address Translation (NAT)

Definido na RFC 2766, esse mecanismo basicamente é capaz transformar um endereço IPv4 em IPv6 (equivalente).

1. Converta o endereço IPv4 para binário;
2. Separe os binários em dois grupos de quatro dígitos;
3. Utilize a base "desejada" para conversão de cada grupo dos binários;
4. Converta os números encontrados em cada um dos grupos para hexadecimal;
5. Adicione o 0 nos cinco primeiros grupos de 16 bits, seguido de FFFF.

IPv6

Os nodos devem possuir algum mecanismo que permita a passagem e o roteamento das mensagens, sendo possível ocorrer:

Nodo IPv4 (IPv4 only node): oferece apenas suporte aos dispositivos que aceitem as configurações com o protocolo IPv4.

Nodo IPv6 (IPv6 only node): tem suporte apenas para prover a comunicação IPv6.

Nodo IPv4/IPv6: possui suporte aos dois protocolos, não necessitando, assim, de nenhuma técnica de transição.

Dessa forma, com exceção do nodo IPv4/IPv6, as demais redes necessitam utilizar alguma técnica para garantir a coexistência e a interoperabilidade entre as duas versões dos protocolos e, consequentemente, o funcionamento correto dos serviços de rede.

IPv6

6to4

Esta foi a primeira técnica adotada para interoperabilidade entre os protocolos IPv4/IPv6. O mecanismo, definido na RFC 3056, permite que redes IPv6 isoladas consigam se comunicar "roteador a roteador" por túnel automático:

Roteadores 6to4: devem encaminhar ambos os endereços dos dispositivos clientes.

Dispositivos clientes: devem estar configurados, pelo menos, com o endereço IPv4.

IPv6

Tunelamento (tunneling)

Determinado pela RFC 2983, fornece orientações técnicas para permitir a utilização de uma infraestrutura IPv4 para encaminhar pacotes IPv6.

São estas as possibilidades:

Roteador a roteador: o pacote IPv6 é encapsulado no início de sua transmissão, dentro de um pacote IPv4, posteriormente tunelado. Assim, quando atingir o seu destino, efetua o desencapsulamento (a mesma regra vale para tunelamento IPv4 para IPv6).

IPv6

Roteador a host: um computador IPv4 envia um pacote a um computador IPv6; o pacote, então, atravessa um roteador com suporte à pilha dupla para assim chegar ao seu destino. Para isso, é necessário um túnel entre o roteador e o computador destino.

Host a host: computadores com pilha dupla se comunicam em uma rede IPv4; para isso, o tunelamento ocorre entre os dois computadores.

IPv6

Túnel broker

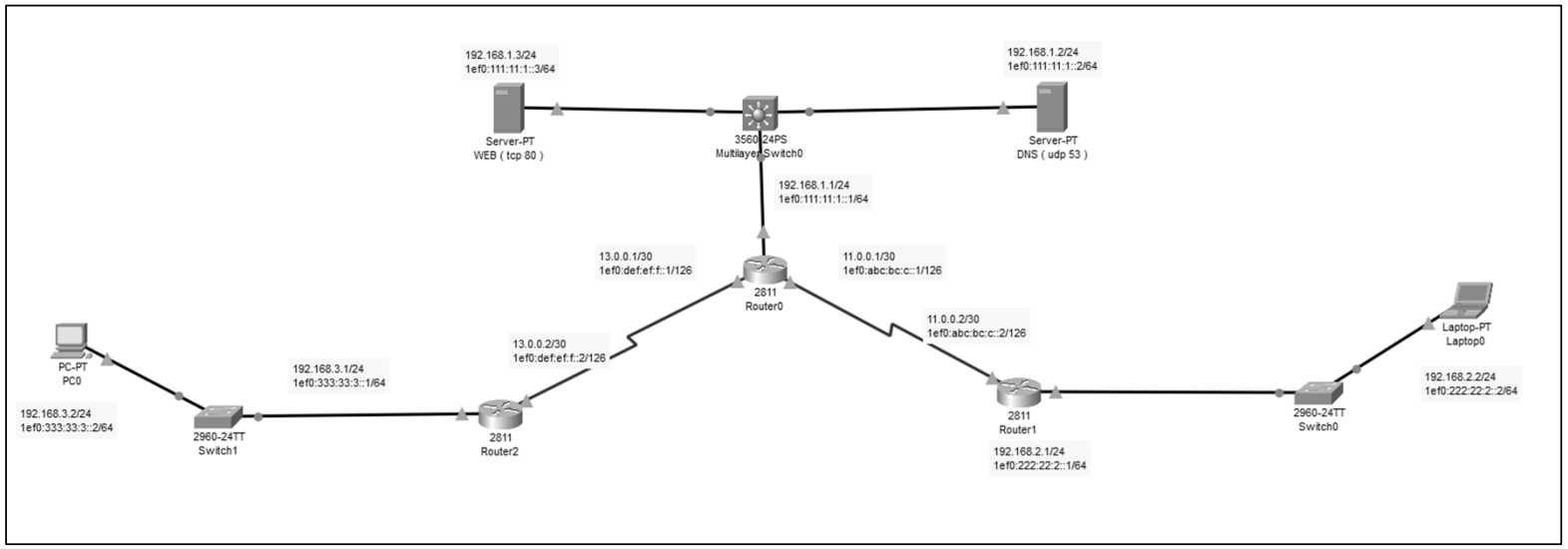
Este mecanismo foi definido na RFC 3035: o pacote IPv6 é encapsulado dentro do pacote IPv4, permitindo o roteamento através do túnel. Essa técnica normalmente é utilizada em sites IPv4/IPv6 ou em computadores que estejam em uma rede IPv4 e necessitem de interoperabilidade em seus acessos.

ISATAP (intra-site automatic tunnel addressing protocol)

Esta técnica foi definida em duas RFCs, sendo elas a 5214 e 4213. Com ela é possível utilizar um endereço atribuído pelo DHCPv4 aos dispositivos, possibilitando que o nodo ISATAP determine a entrada e a saída do túnel IPv6.

Princípios de comunicação de dados e teleprocessamento

EXERCÍCIO 01:



Princípios de comunicação de dados e teleprocessamento

Em diversas situações, o administrador de redes necessita dividir a sua rede em diversas sub-redes, a fim de isolar os departamentos para garantia de integridade, gerenciamento centralizado dos recursos, entre outras necessidades. Para isso, os administradores de redes utilizam as técnicas como o cálculo de sub-redes por meio da manipulação da máscara de rede. Para utilizar as técnicas de sub-redes, por meio da alteração da máscara de sub-redes, é necessário conhecer a máscara padrão utilizada.

Classe	Máscara padrão
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Assinale a alternativa que represente corretamente a porção destinada à rede e aos hosts da classe B:

a) Rede.Rede.Rede.Rede

b) Rede.Rede.Rede.Host

c) Host.Host.Host.Host

d) Rede.Host.Host.Host

e) Rede.Rede.Host.Host

Na maioria das empresas existem redes de computadores que visam garantir que os recursos sejam compartilhados e diversos serviços sejam providos. Esse tipo de rede pode ser considerado uma rede local (LAN – local area network), caracterizando, assim, uma típica rede Ethernet. Com base no contexto apresentado anteriormente, observe as afirmativas a seguir:

I. A rede do tipo Ethernet, pode ser definida como Norma 802.8.

II. Na rede Ethernet os dispositivos devem estar conectados em uma mesma linha de comunicação.

III. Os meios de ligação da rede Ethernet devem ser constituídos por cabos cilíndricos.

Assinale a alternativa correta:

a) Somente a afirmativa II é verdadeira.

b) Somente as afirmativas II e III são verdadeiras.

c) Somente as afirmativas I e III são verdadeiras.

d) Somente a afirmativa III é verdadeira.

e) Somente as afirmativas I e II são verdadeiras

No final dos anos 1970, quando os engenheiros estavam projetando o IP (Internet Protocol), não se previa que haveria diversos serviços disponíveis na rede mundial de computadores. Esses e outros motivos contribuíram significativamente para a escassez de endereços. Com base nisso, a IETF projetou e desenvolveu um novo protocolo que atendesse às novas demanda das redes, o IPv6. Inicialmente, a intenção da IETF era suprir a necessidade de endereço, razão pela qual o protocolo IPv6 foi projetado com 128 bits, divididos em oito grupos com quatro dígitos hexadecimal. Dessa forma, a quantidade possível de endereçamento é de:

a) 2^{128}, ou seja, 34 undecilhões.

b) 2^{32}, ou seja, 40 undecilhões.

c) 2^{128}, ou seja, 340 undecilhões.

d) 128^{2}, ou seja, 3 undecilhões.

e) 2^{12}, ou seja, 30 undecilhões

Princípios de comunicação de dados e teleprocessamento

Em diversas situações, o administrador de redes necessita dividir a sua rede em diversas sub-redes, a fim de isolar os departamentos para garantia de integridade, gerenciamento centralizado dos recursos, entre outras necessidades. Para isso, os administradores de redes utilizam as técnicas como o cálculo de sub-redes por meio da manipulação da máscara de rede. Para utilizar as técnicas de sub-redes, por meio da alteração da máscara de sub-redes, é necessário conhecer a máscara padrão utilizada.

Classe	Máscara padrão
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Assinale a alternativa que represente corretamente a porção destinada à rede e aos hosts da classe B:

a) Rede.Rede.Rede.Rede

b) Rede.Rede.Rede.Host

c) Host.Host.Host.Host

d) Rede.Host.Host.Host

e) Rede.Rede.Host.Host

Na maioria das empresas existem redes de computadores que visam garantir que os recursos sejam compartilhados e diversos serviços sejam providos. Esse tipo de rede pode ser considerado uma rede local (LAN – local area network), caracterizando, assim, uma típica rede Ethernet. Com base no contexto apresentado anteriormente, observe as afirmativas a seguir:

I. A rede do tipo Ethernet, pode ser definida como Norma 802.8.

II. Na rede Ethernet os dispositivos devem estar conectados em uma mesma linha de comunicação.

III. Os meios de ligação da rede Ethernet devem ser constituídos por cabos cilíndricos.

Assinale a alternativa correta:

a) Somente a afirmativa II é verdadeira.

b) Somente as afirmativas II e III são verdadeiras.

c) Somente as afirmativas I e III são verdadeiras.

d) Somente a afirmativa III é verdadeira.

e) Somente as afirmativas I e II são verdadeiras

No final dos anos 1970, quando os engenheiros estavam projetando o IP (Internet Protocol), não se previa que haveria diversos serviços disponíveis na rede mundial de computadores. Esses e outros motivos contribuíram significativamente para a escassez de endereços. Com base nisso, a IETF projetou e desenvolveu um novo protocolo que atendesse às novas demanda das redes, o IPv6. Inicialmente, a intenção da IETF era suprir a necessidade de endereço, razão pela qual o protocolo IPv6 foi projetado com 128 bits, divididos em oito grupos com quatro dígitos hexadecimal. Dessa forma, a quantidade possível de endereçamento é de:

a) 2^{128}, ou seja, 34 undecilhões.

b) 2^{32}, ou seja, 40 undecilhões.

c) 2^{128}, ou seja, 340 undecilhões.

d) 128^{2}, ou seja, 3 undecilhões.

e) 2^{12}, ou seja, 30 undecilhões

Recapitulando

Recapitulando

- Redes e sub-redes;
- Ethernet;
- IPv6.