

# **Redes e Sistemas Distribuídos**

**Arquitetura e tecnologia de redes**

Prof. Dr. Gilberto Fernandes Junior

- Unidade de Ensino: 2
- Competência da Unidade: Conhecer o endereço IP e suas atribuições, sub-redes e a Ethernet, bem como, a diferenciar as arquiteturas e a otimizar os recursos disponíveis, a partir do gerenciamento das redes.
- Resumo: Análise de arquiteturas de redes
- Palavras-chave: rede, IP, arquitetura, gerência
- Título da Teleaula: Arquitetura e tecnologia de redes
- Teleaula nº: 2

# Contextualização

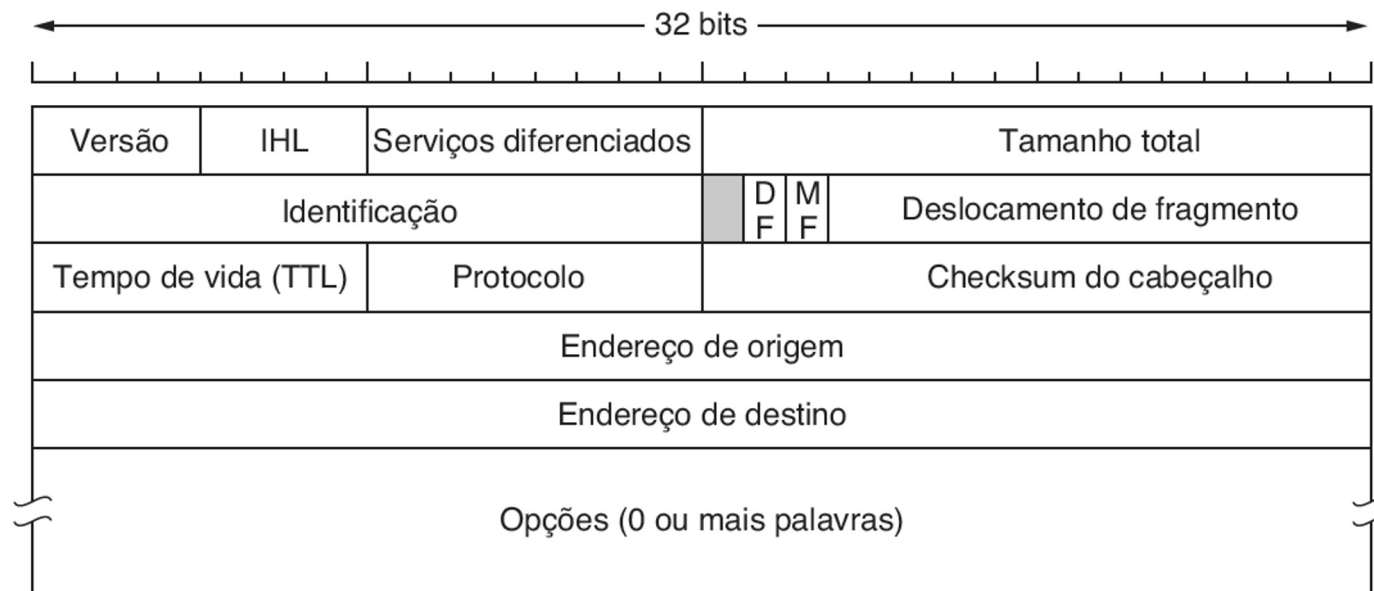
- Redes e sub-redes
- Ethernet
- IPv4 e IPv6
- Gerência de desempenho, configuração e contabilização

# **Protocollo IPv4**

## *Internet protocol (IP)*

- O *Internet Protocol* (IP) é o endereço lógico feito para que um dispositivo possa se comunicar com qualquer outro dispositivo, independentemente de sua localização geográfica.
- RFC 791 (versão 4) – IPv4
- 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

# Datagrama Ipv4



Fonte: TANENBAUM, A. S. Redes de Computadores. 5. ed. São Paulo: Pearson, 2011.

# Notação do IPv4

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

- Exemplo

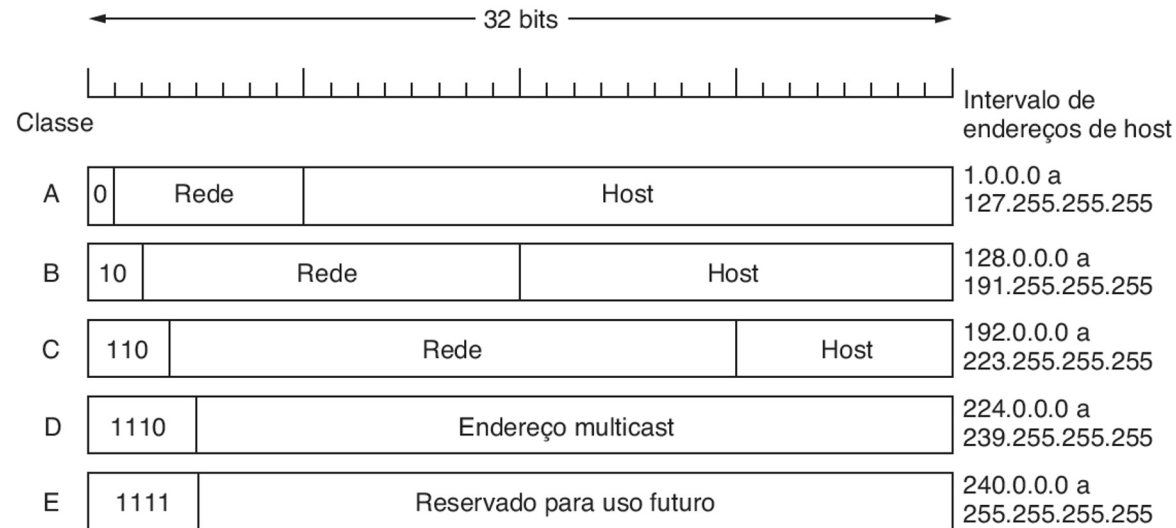
**172.16.30.110**

**172.16** → identifica à qual rede o dispositivo pertence.

**30.110** → determina o endereço do dispositivo.

# Classes de endereço

- Os endereçamentos utilizados nas redes foram divididos em classes para utilização de acordo com o número de dispositivos da rede





# DNS (*Domain Name System*)

- Sistema de Nomes de Domínios
- Efetuar a tradução do número IP (Internet Protocol) para o nome de domínios, dentro de um servidor DNS
- Exemplo: www.google.com -> 172.217.172.131
- **Domínio genérico:** Registros conforme o segmento do site (.com, .net, .org, .edu, .gov, entre outros)
- **Domínio de países:** br (Brasil), us (Estados Unidos),
- **Domínio reverso:** processo reverso à consulta ao servidor DNS.

# **Sub-Redes**

# Sub-rede

- Quando um pacote entra no roteador principal de uma rede classe B, como este sabe para qual sub-rede (Ethernet) deve entregar o pacote?
  - tabela com 65.536 entradas? Não!
  - Alguns bits são retirados do número do host para criar um número de sub-rede.
  - Roteador precisa de uma máscara de sub-rede

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

# Sub-rede

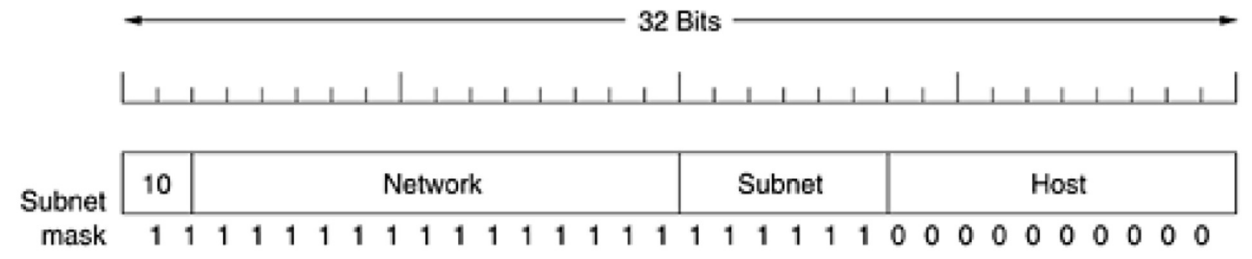
- Permitir que uma rede seja dividida em diversas partes para uso interno, mas externamente continue a funcionar como uma única rede.

## **Vantagens:**

- Redução do tráfego de rede
- Simplificação no gerenciamento da rede
- Controle dos recursos da rede

# Sub-rede: Exemplo

- Uma rede de classe B dividida em 64 sub-redes



Sub-rede 1: 10000010 00110010 000001|00 00000001  
Sub-rede 2: 10000010 00110010 000010|00 00000001  
Sub-rede 3: 10000010 00110010 000011|00 00000001

Fonte: Adaptado de: TANENBAUM, A. S. Redes de computadores. 4 ed. Rio de Janeiro: Campus, 1997

# Cálculo de sub-rede e máscara de sub-rede

- Rede de classe C: 192.168.0.0
- Máscara padrão: 255.255.255.0
- 255.255.255.0  $\rightarrow$  11111111.11111111.11111111.00000000
- Rede:  $2^n = 2^2 = 4$  ,
- Hosts por sub-rede:  $2^n = 2^6$  64
- Nova máscara: 11111111.11111111.11111111.**11**000000
- = 255.255.255.192
- Notação CIDR: 192.168.0.3 /**26**

# Cálculo de sub-rede e máscara de sub-rede

Rede	1º IP válido	Último 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

Tabela de sub-redes

192.168.0.66 = 11000000.10101000.00000000.01000010

**AND**

255.255.255.192 = 11111111.11111111.11111111.11000000

**= Endereço da REDE:**

192.168.0.64 = 11000000.10101000.00000000.01000000

# Ethernet



# Ethernet

Pode se definir Ethernet como um padrão utilizado em transmissões em redes locais (Norma IEEE 802.3)

- Conexão dos dispositivos: devem estar conectados em uma mesma linha de comunicação.
- Meios de ligação: devem ser constituídas por cabos cilíndricos

# Ethernet

O tipo de tecnologia do cabeamento dita a velocidade que cada um deles pode atingir:

- Fast Ethernet (802.3u): 100 Mbit/s. 100Base-TX, 100Base-T e 100Base-FX.
- Gigabit Ethernet (802.3z): 1 Gigabit/s. 1000BASE-LX, 1000BASE-SX, 1000BASE-CX e 1000BASE-T.
- 10 Gbit/s Ethernet (802.3ae)
- 40/100 Gbit/s Ethernet (802.3)

# Métodos de transmissão Ethernet

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.

# Métodos de transmissão Ethernet

## **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

- CSMA não persistente: se o meio estiver ocupado, o dispositivo espera um tempo aleatório
- CSMA 1 persistente: dispositivo “escuta” a rede até que o meio fique livre
- CSMA p-persistente: calcula a probabilidade de colisão

# Métodos de transmissão Ethernet

## **CD (*collision 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 Computada**

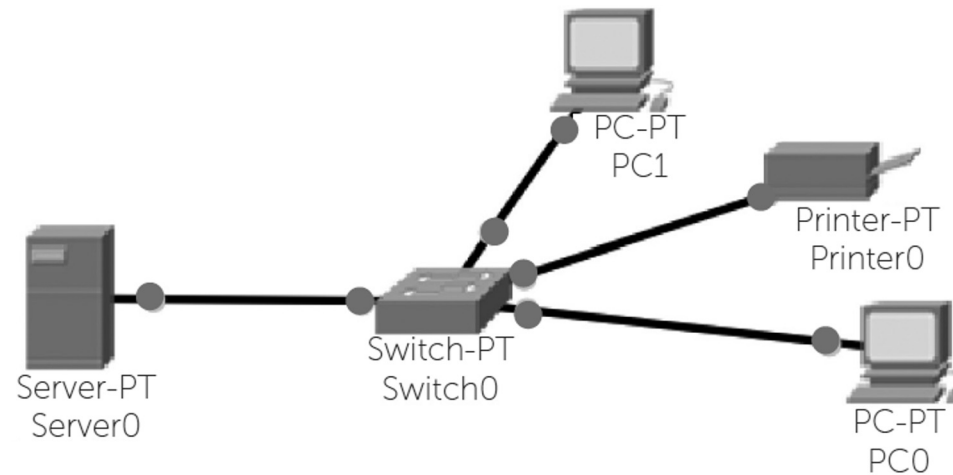
# Ethernet comutada

As transmissões 802.3 utilizam um cabeçalho de 14 bytes, dos quais:

- 6 bytes: são utilizados para o endereço de origem.
  - 6 bytes: são para o endereço de destino.
  - 2 bytes: descrevem o número total de bytes a serem transmitidos.
- 
- É constituída em cima de uma topologia estrela

# Ethernet comutada

Exemplo:



Fonte: Retirado de: Nunes, Sergio Eduardo. Redes de computadores. Londrina : Editora e Distribuidora Educacional S.A. 2017.

*\*outros tipos de topologia, como em barramento, não se permitem tais velocidades*



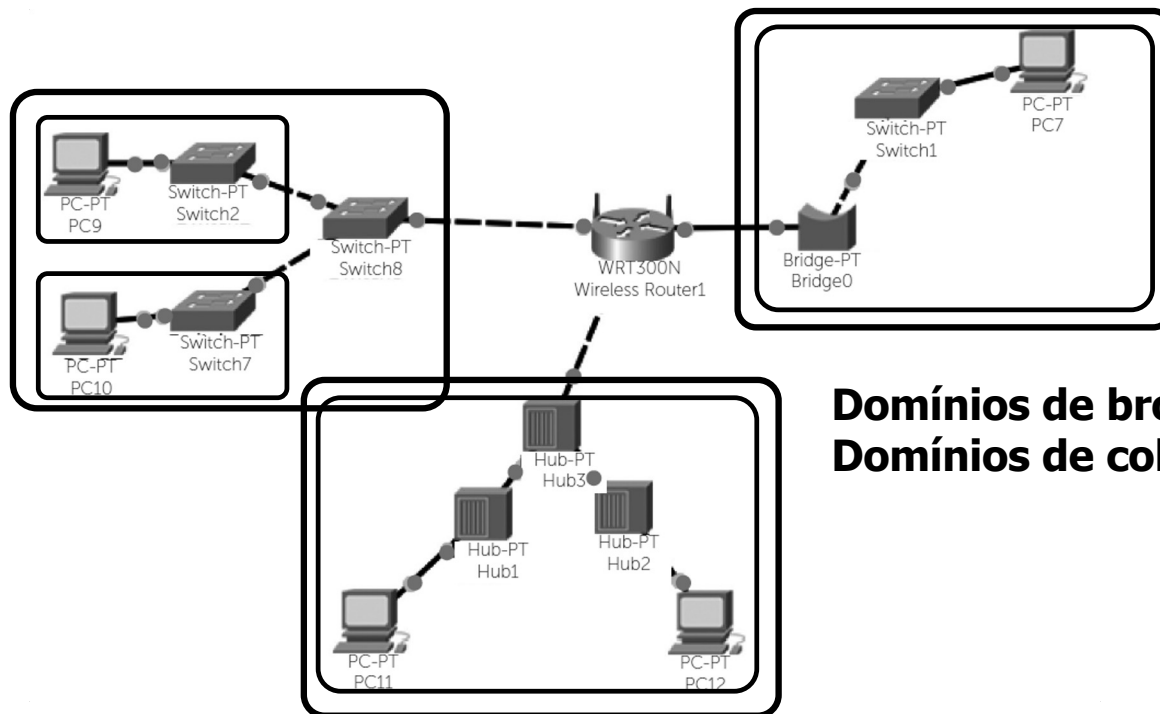
# Domínio de colisão

- 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 cascadeado, a rede pode sofrer maiores consequências.

# Domínio de broadcast

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

# Domínio de colisão e de broadcast



**Domínios de broadcast: 3**  
**Domínios de colisão: 4**

Fonte: Adaptado de: Nunes, Sergio Eduardo. Redes de computadores. Londrina: Editora e Distribuidora Educacional S.A. 2017.

**Qual o intuito de  
desenvolver redes em  
sub-redes?**

**IPv6**

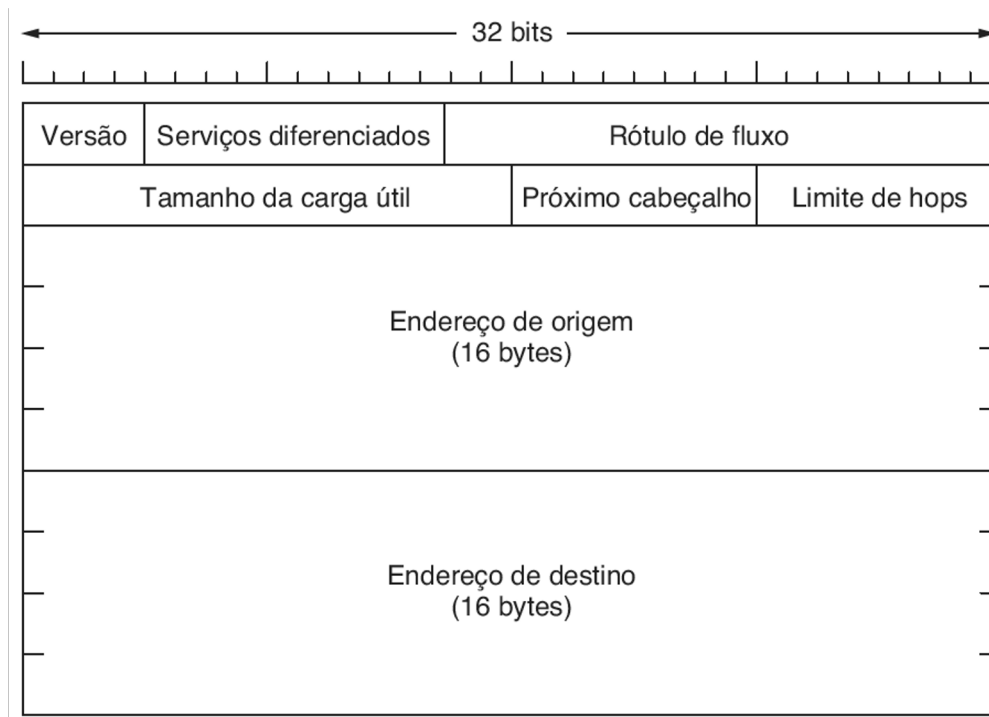
# IPv6

- Popularização da Internet – esgotamento do protocolo IPv4
- IPv6 teve início em 1990
- Empresas como Google, Yahoo e Facebook iniciaram a migração para o protocolo IPv6 em 2010
- Possui 128 bits (340 undecilhões de endereços)
- Oito grupos com quatro dígitos hexadecimais:  
8000:0000:0010:0000:0123:4567:89AB

# IPv6

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

# Cabeçalho IPv6



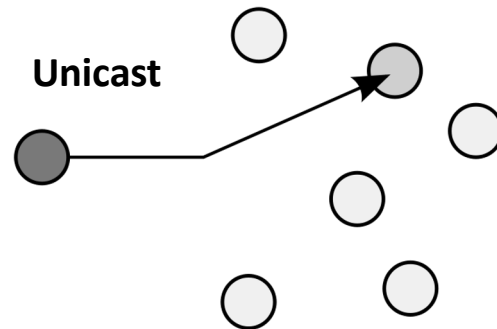
Fonte: TANENBAUM, A. S. Redes de Computadores. 5. ed. São Paulo: Pearson, 2011. pág. 287



# Tipos de Endereçamento IPv6

## Unicast

- Identifica uma única interface
- Global-Unicast, Link-Local (FE80:: /64) e Unique-Local (FC00:: /7)

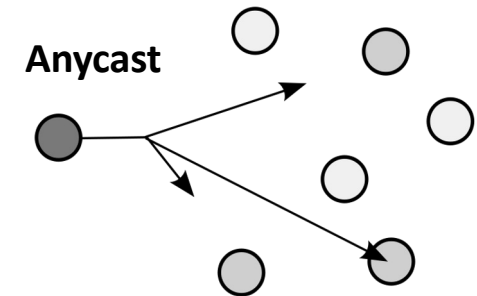


Fonte: elaborado pelo autor

# Tipos de Endereçamento IPv6

## Anycast

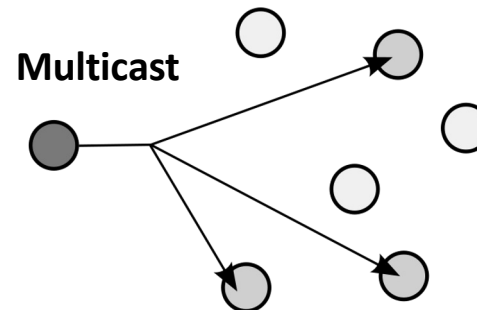
- identificam um grupo de interfaces de nós diferentes
- O pacote alcança a interface mais próxima



Fonte: elaborado pelo autor

## Multicast

- Identifica um grupo de interfaces ou grupo de nós.
- O pacote alcança todas as interfaces do grupo



Fonte: elaborado pelo autor

# Coexistência e Interoperabilidade

- Toda a estrutura da Internet está baseada no IPv4.
- Uma troca imediata de protocolo é inviável devido o tamanho e a proporção que esta rede possui.
- A adoção do IPv6 deve ser realizada de forma gradual.
- Haverá inicialmente um período de transição e de coexistência entre os dois protocolos.
- Redes IPv4 precisarão comunicar-se com redes IPv6 e vice-versa.
- Técnicas que visam manter a compatibilidade

# IPv4 vs IPv6

Versão / Itens	IPv4	IPv6
Quantidade de endereços	$2^{32}$	$2^{128}$
Quantidade de campos	14	8
MTU mínimo	576 bytes	1280 bytes
Representação do endereço	4 grupos de 8 bits	8 grupos de 16 bits
Tamanho do endereço	32	128
Roteamento	Tabela de roteamento	Efetutado pelo cabeçalho de extensão
Segurança	IPSec facultativo	IPSec obrigatório
Qualidade de Serviço (QoS)	Sem garantia	Através dos campos, classe de tráfego e identificação de fluxo
Cabeçalho	Uso do checksum	Mais simplificado

Fonte: elaborado pelo autor

# **Técnicas de Transição IPv4 / IPv6**

# Descrição da SP

- A NET@RTG é uma empresa especializada em redes
- Um dos seus clientes provê jogos on-line, razão pela qual tem a necessidade de ter diversos servidores espalhados pelos países.
- Um dos seus servidores apresentou indisponibilidade: ao abrir um chamado foi indicada a necessidade de um mecanismo de transição em sua topologia.
- Uma vez que esse cliente é de sua responsabilidade, o diretor de TI solicitou a você que **descreva os mecanismos de transição disponíveis!**

# Técnicas de transição

## **Pilha Dupla**

- Provê o suporte a ambos os protocolos no mesmo dispositivo.
- A mensagem está no formato IPv4 e é encapsulada com IPv6, ou vice-versa

# Técnicas de transição

## **Tunelamento (*tunneling*)**

- Determinado pela RFC 2983, fornece orientações técnicas para permitir a utilização de uma infraestrutura IPv4 para encaminhar pacotes IPv6.
- Possibilidades
  - Roteador a roteador
  - Roteador a *host*
  - *Host a host*



# Técnicas de transição

## **Túnel *broker***

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

# Técnicas de transição

## **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

# **Gerência de Desempenho, Configuração e Contabilização**

# Introdução

- Todos nós já utilizamos algum meio de ou um serviço de rede, que não conseguiu atender com a qualidade esperada.
- Para que possamos parametrizar alguns serviços, é necessário conhecermos quais são os indicadores utilizados nas redes de computadores a fim de garantir a qualidade e a disponibilidade.

# Gerência de Redes

## **Nível de utilização**

- testes de desempenho por meio da injeção de um determinado tráfego na rede,
  - Taxa máxima suportada, Tempo de deslocamento de um pacote, Tempo de recuperação a falhas.

## **Perfil de tráfego**

- ao conhecer o perfil do tráfego da rede, é possível adequar os recursos às necessidades, ou ainda manter o equilíbrio necessário para ter um nível de qualidade adequado.

# Gerência de Redes

## **Vazão ( *Throughput* )**

- quantidade de dados transferidos entre dispositivos em determinado tempo - bits por segundo (bps).
- taxa de transferência pode ser menor do que a largura de banda, devido a perdas e atrasos.

## **Perda de pacotes**

- roteadores não tem capacidade de armazenamento de pacotes infinita,
- após o esgotamento, os pacotes são descartados.

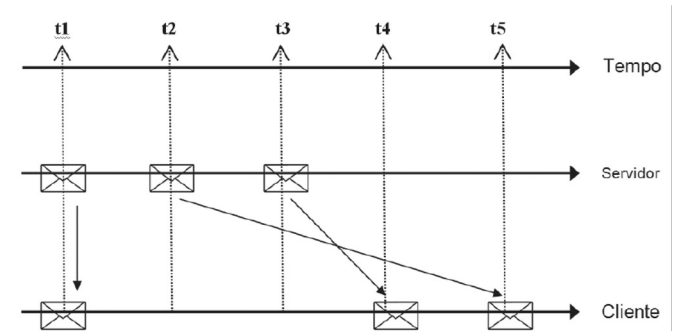
# Gerência de Redes

## Latência (atraso)

- Tempo de transmissão + Tempo de propagação
  - Tempo de transmissão =  $\text{Dimensão do pacote (bits)} / \text{Velocidade da Transmissão (bps)}$ .
  - Tempo de propagação =  $\text{Dimensão do Canal (Km)} / \text{Velocidade de Propagação (Km/s)}$ .

## Jitter

- variação no tempo e na sequência de entrega dos pacotes (Packet-Delay Variation) devido à variação da latência (atrasos) na rede



Fonte: Adaptado de: Nunes, Sergio Eduardo. Redes de computadores. Londrina: Editora e Distribuidora Educacional S.A. 2017.

# Gerência de Redes

## **Disponibilidade**

- Capacidade que equipamentos e redes possuem de forma contínua por um período.
- $D = \text{MTTF} / (\text{MTTF} + \text{MTTR})$ 
  - Tempo médio para falhas (MTTF) e Tempo médio para reparos (MTTR)

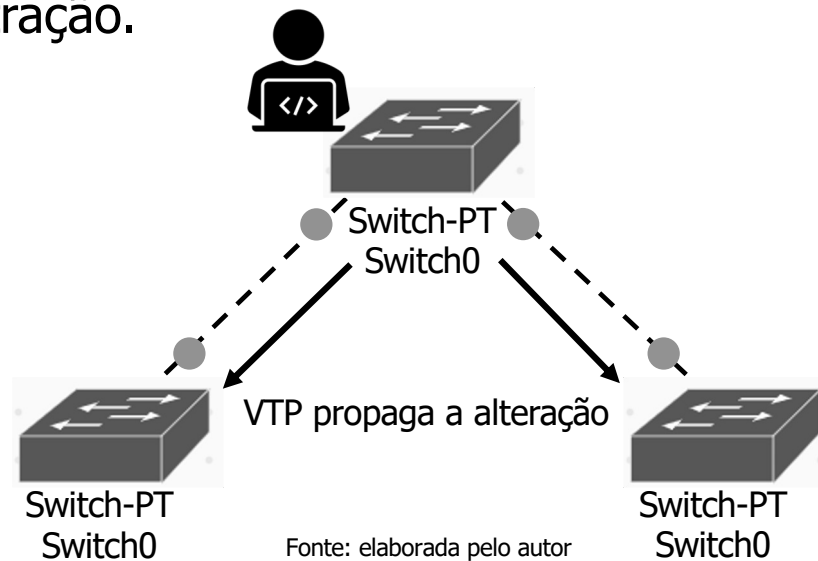
## **QoS ( *Quality of Service* – Qualidade de Serviço)**

- conjunto de regras, mecanismos e tecnologias que tem o propósito de utilizar os recursos disponíveis de forma eficaz e econômica.



# VLAN Trunk Protocol

- Protocolo de camada 2, desenvolvido pela Cisco, para configuração de VLANs, facilitando, assim, a sua administração.



# **Acesso Remoto: Servidor SSH**

# Descrição da SP

- Você é um administrador de rede e uma universidade e possui um servidor linux configurado para capturar o tráfego de rede, a fim de entender o perfil de tráfego e possibilitar a detecção de erros e anomalias de tráfego.
- Como você está trabalhando em Home Office durante um período, é necessário configurar uma forma de **acesso remoto** ao servidor para eventuais configurações e verificações. **Como isso pode ser realizado?**

# Resolução da SP

## **SSH (*Secure Socket Shell*)**

- é um protocolo de rede que permite aos usuários acessar e gerenciar servidores pela internet.
- Utiliza criptografia
- Putty – cliente SSH no Windows

**Dúvidas?**

**Recapitulando**

# Recapitulando

- Redes e sub-redes
- Ethernet
- IPv4 e IPv6
- Gerência de desempenho, configuração e contabilização
- Acesso remoto com SSH