TIC

AULA 16

PROF: ROBERTO

O QUE VAMOS VER NESSA AULA

- IPv6:
  - Conceitos:
    - Motivação;
    - Características;
    - Comparação;
    - Abreviação.
- QOS
- VPN
- Avaliação

1.

IPV6

Características

INTRODUÇÃO AO IPV6

Motivação para o IPv6:

- **Escassez de endereços IPv4:** O IPv4 utiliza endereços de 32 bits, o que limita a quantidade de endereços possíveis (4.3 bilhões de endereços), que já estão quase totalmente esgotados.

- **IPv6** foi criado para resolver esse problema, utilizando endereços de 128 bits, o que permite cerca de 340 undecilhões de endereços (mais do que suficiente para a internet futura).

INTRODUÇÃO AO IPV6 - CARACTERÍSTICAS

- **Endereços de 128 bits:** Comparado aos 32 bits do IPv4, os endereços IPv6 são muito maiores.
- **Simplificação de cabeçalhos:** O cabeçalho do IPv6 é mais simples e eficiente do que o do IPv4, facilitando o roteamento.
- **Autoconfiguração (SLAAC):** Os dispositivos podem se autoconfigurar em uma rede sem a necessidade de um servidor DHCP, utilizando o Router Advertisement (RA).
- **Link-Local Addresses:** IPv6 utiliza endereços link-local (fe80::/64) para comunicação dentro da mesma rede local, sem precisar de um roteador.

INTRODUÇÃO AO IPV6 - FORMATO

Notação:

- O endereço IPv6 é representado em formato hexadecimal, dividido em grupos de 4 dígitos separados por dois-pontos.
  - **Exemplo:** 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

Abreviação de endereços:

- Abreviação ::: Zeros consecutivos podem ser omitidos usando :: (só pode ser utilizado uma vez no endereço).
  - **Exemplo:** 2001:0db8:85a3::8a2e:0370:7334 (em vez de colocar zeros no meio).
- Remoção de zeros à esquerda: Zeros à esquerda podem ser omitidos em cada grupo hexadecimal.
  - **Exemplo:** 2001:db8:85a3::1.

INTRODUÇÃO AO IPV6 - FORMATO

Notação:

- O endereço IPv6 é representado em formato hexadecimal, dividido em grupos de 4 dígitos separados por dois-pontos.
  - **Exemplo:** 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

Abreviação de endereços:

- Abreviação ::: Zeros consecutivos podem ser omitidos usando :: (só pode ser utilizado uma vez no endereço).
  - **Exemplo:** 2001:0db8:85a3::8a2e:0370:7334 (em vez de colocar zeros no meio).
- Remoção de zeros à esquerda: Zeros à esquerda podem ser omitidos em cada grupo hexadecimal.
  - **Exemplo:** 2001:db8:85a3::1.
    - 2001:0db8:85a3:0000:0000:0000:0000:0001

INTRODUÇÃO AO IPV6 - TIPOS DE ENDEREÇOS IPV6

- **Unicast Global:** Usado para comunicação unicast (um para um) na internet pública. Começa normalmente com 2000::/3.
- **Link-Local (fe80::):** Usado para comunicação dentro da rede local, entre dispositivos conectados diretamente.
- **Unique Local Address (ULA):** Funciona de forma similar aos endereços privados do IPv4. Inicia com fc00::/7.
- **Multicast:** Usado para comunicação com múltiplos dispositivos simultaneamente. Começa com ff00::/8.
- **Anycast:** Um único endereço que pode ser atribuído a múltiplos dispositivos. O roteador encaminha o tráfego para o dispositivo mais próximo.

INTRODUÇÃO AO IPV6 - AUTOCONFIGURAÇÃO DE IPV6

Stateless Address Autoconfiguration (SLAAC):

- O SLAAC permite que os dispositivos autoconfigurem seus próprios endereços IPv6. Os roteadores enviam mensagens **Router Advertisement (RA)** que contêm o prefixo de rede, e os dispositivos criam seu próprio endereço IPv6 usando esse prefixo e o ID de interface (normalmente derivado do MAC Address).

DHCPv6:

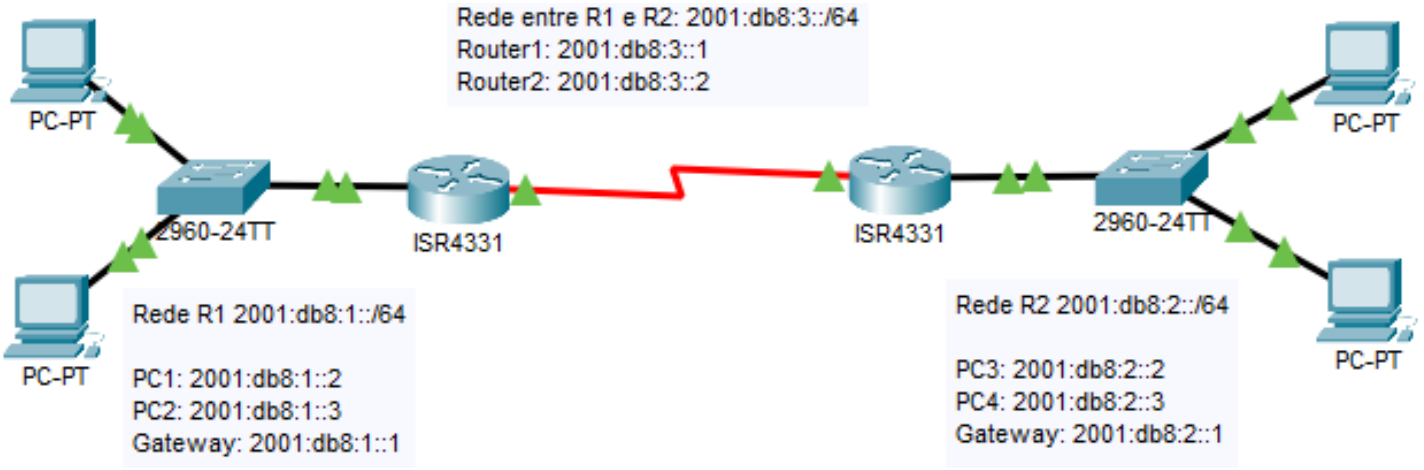
- No **DHCPv6**, o servidor atribui endereços IPv6 aos clientes, semelhante ao IPv4, mas também pode complementar o SLAAC enviando configurações adicionais como DNS e opções de roteador.

2.

SIMULANDO

IPv6

IPV6 - EXEMPLO



IPV6 - EXEMPLO - SOLUÇÃO

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#int gi 0/0/0
R1(config-if)#ipv6 address 2001:db8:1::1/64
R1(config-if)#no shut

R1(config-if)#exit
R1(config)#int serial 0/1/0
R1(config-if)#ipv6 add 2001:db8:3::1/64
R1(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
R1(config-if)#exit
R1(config)#ipv6 unicast-routing
R1(config)#ipv6 route 2001:db8:2::/64 2001:db8:3::2
R1(config)#exit
```

2001:db8:3::2 é o endereço IPv6 atribuído à interface.
/64 indica o tamanho do prefixo de rede, ou seja, os primeiros 64 bits identificam a rede, e os 64 bits restantes identificam o host dentro dessa rede.

Roteamento IPv6

IPV6 - EXEMPLO - SOLUÇÃO

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R2
R2(config)#int gi 0/0/0
R2(config-if)#ipv6 address 2001:db8:2::1/64
R2(config-if)#no shut

R2(config-if)#exit
R2(config)#int serial 0/1/0
R2(config-if)#ipv6 add 2001:db8:3::2/64
R2(config-if)#no shut

R2(config-if)#exit
R2(config)#ipv6 unicast-routing
R2(config)#ipv6 route 2001:db8:1::/64 2001:db8:3::1
R2(config)#exit
```

3.

QOS

IPv6

QOS - INTRODUÇÃO

- **QoS (Quality of Service)** refere-se ao gerenciamento de recursos de rede para garantir a qualidade de voz, vídeo, e dados em uma rede.
- Permite priorizar certos tipos de tráfego de rede com base em requisitos de desempenho.

- **Objetivos da QoS:**
  - Garantir largura de banda para aplicações críticas.
  - Controlar jitter e latência para chamadas de voz e vídeo.
  - Minimizar perda de pacotes e atrasos.

QOS - IMPORTANCIA

- Redes corporativas modernas transportam diferentes tipos de tráfego: voz, vídeo, e dados.
- Sem QoS, serviços como VoIP ou vídeo podem ser degradados por congestionamento de rede.
- QoS é usada para garantir que o tráfego sensível a atrasos, como voz e vídeo, tenha prioridade.

QOS – MODELOS DE QOS

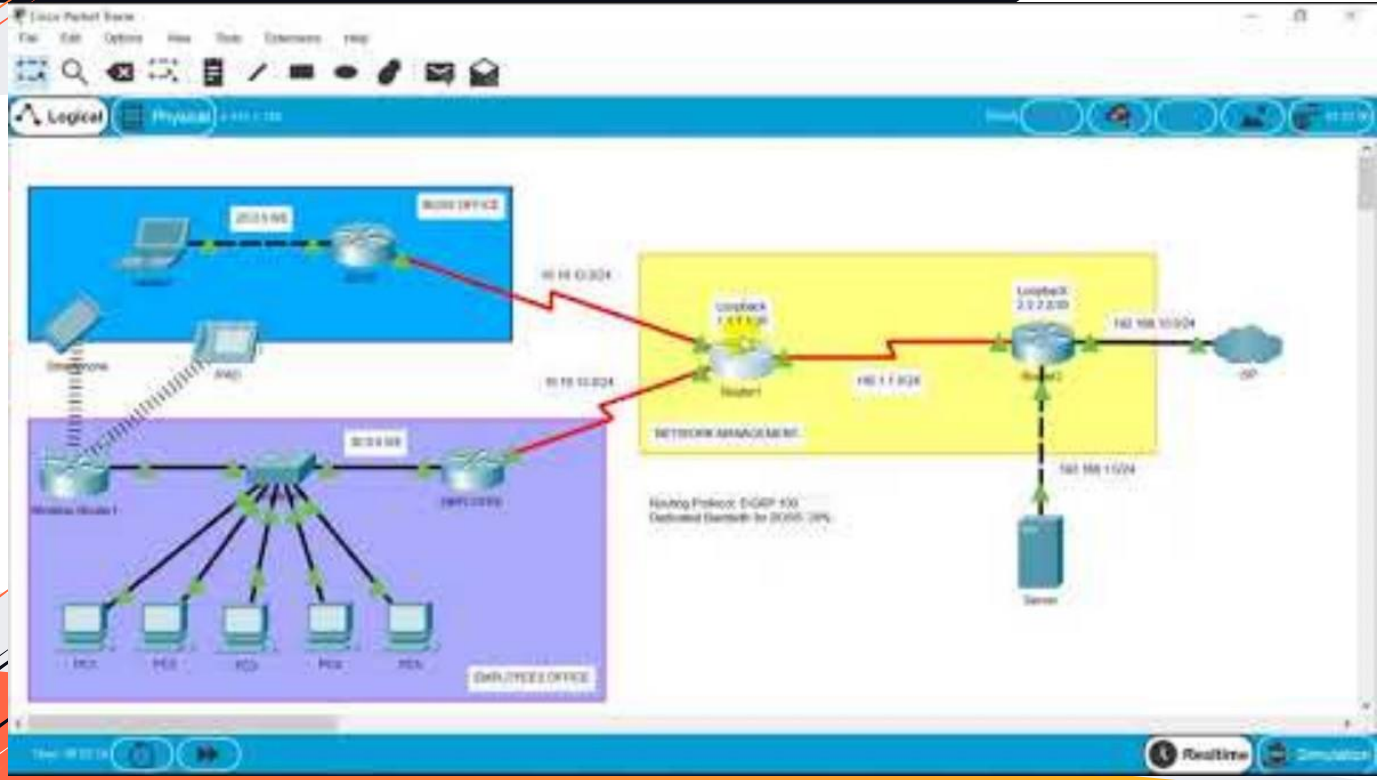
Existem três principais modelos de QoS usados em redes:

- **Best-Effort:** Sem garantias de qualidade.
- **Integrated Services (IntServ):** Fornece reservas explícitas de recursos para fluxos específicos.
- **Differentiated Services (DiffServ):** Usa marcações nos pacotes para tratar fluxos de tráfego de forma diferenciada.

QOS – CLASSIFICAÇÃO E MARCAÇÕES DE PACOTES

- A classificação de pacotes permite identificar e tratar o tráfego de forma diferenciada.
- Os pacotes podem ser marcados com:
  - **IP Precedence:** Definido em 3 bits no cabeçalho IP.
  - **DSCP (Differentiated Services Code Point):** Usa 6 bits para definir a prioridade do tráfego.

QOS – CLASSIFICAÇÃO E MARCAÇÕES DE PACOTES



https://www.youtube.com/watch?v=Ur55nyokzN4

3.

VPN

conceitos

VPN – VIRTUAL PRIVATE NETWORK

- VPN (Virtual Private Network) é uma tecnologia que cria uma conexão segura e criptografada entre duas redes ou entre um dispositivo e uma rede, usando uma rede pública, como a Internet.

- **Objetivo:** Proteger a privacidade e a integridade dos dados enquanto trafegam entre redes ou dispositivos remotos, como se estivessem na mesma rede local.

VPN – VIRTUAL PRIVATE NETWORK - TIPOS

VPN Site-to-Site:

- Conecta redes inteiras em locais diferentes.
- Usada por empresas para unir escritórios geograficamente distantes como se estivessem na mesma rede.

VPN de Acesso Remoto:

- Permite que um usuário se conecte a uma rede corporativa de forma segura de qualquer lugar.
- Ideal para funcionários que trabalham remotamente e precisam acessar recursos da rede da empresa.

VPN – VIRTUAL PRIVATE NETWORK - TIPOS

VPN MPLS (Multiprotocol Label Switching):

- Utilizada principalmente por ISPs e em ambientes corporativos para rotear pacotes de dados de forma mais eficiente.

VPN SSL/TLS:

- Comumente usada para acesso seguro à Internet. Os navegadores suportam esse tipo de VPN, ideal para uso em acesso remoto.

VPN – VIRTUAL PRIVATE NETWORK - PROTOCOLOS

- **IPSec:** Protocolo que garante segurança para a comunicação de dados ao fornecer autenticação e criptografia.
- **SSL/TLS:** Usado principalmente para VPN de acesso remoto em navegadores da web.
- **PPTP (Point-to-Point Tunneling Protocol):** Um dos protocolos de VPN mais antigos e mais fáceis de configurar, mas com limitações de segurança.
- **L2TP (Layer 2 Tunneling Protocol):** Geralmente usado com IPSec para aumentar a segurança.
- **GRE (Generic Routing Encapsulation):** Protocolo de encapsulamento simples que pode ser usado junto com IPSec para VPNs de site-to-site.

VPN – VIRTUAL PRIVATE NETWORK - BENEFÍCIOS

- **Segurança:** Criptografia de dados durante o tráfego pela rede pública, protegendo contra interceptações.
- **Privacidade:** Esconde o endereço IP real e protege o tráfego de rede, garantindo o anonimato.
- **Acesso Remoto:** Permite que usuários acessem a rede corporativa de qualquer lugar.
- **Redução de Custos:** Reduz a necessidade de links dedicados caros, permitindo que as empresas usem a infraestrutura de internet existente para conectar sites.

VPN – VIRTUAL PRIVATE NETWORK - FUNCIONAMENTO

- **Criptografia:** Os dados são criptografados no ponto de origem e descriptografados no ponto de destino, garantindo que ninguém no meio do caminho possa entender o conteúdo.

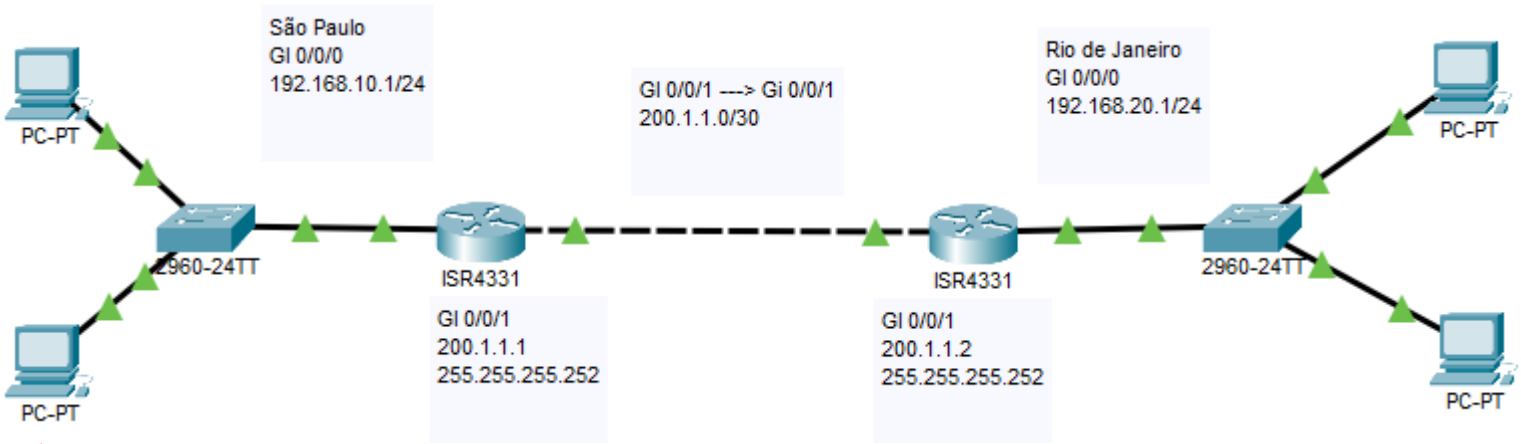
- **Tunelamento:** Os dados viajam por um túnel virtual seguro, criado através de protocolos de tunelamento (por exemplo, IPSec, GRE), para esconder o tráfego de rede dos olhos de terceiros.

- **Autenticação:** Os usuários e dispositivos devem ser autenticados antes de estabelecer uma conexão VPN, o que evita acesso não autorizado.

VPN – VIRTUAL PRIVATE NETWORK - FERRAMENTAS

- **Hardware:** Muitos roteadores Cisco, por exemplo, têm suporte nativo para VPN.
- **Software:** Programas como OpenVPN, Cisco AnyConnect, entre outros, permitem configurar conexões VPN seguras.
- **Serviços:** Existem serviços de VPN de terceiros, como NordVPN, ExpressVPN, entre outros, que oferecem uma solução de privacidade para usuários finais.

VPN – SIMULANDO



VPN - SOLUÇÃO

```
SAO-PAULO(config)#crypto isakmp policy 10
SAO-PAULO(config-isakmp)#authentication pre-share
SAO-PAULO(config-isakmp)#encryption aes
SAO-PAULO(config-isakmp)#hash sha
SAO-PAULO(config-isakmp)#group 2
SAO-PAULO(config-isakmp)#exit
SAO-PAULO(config)#
SAO-PAULO(config)#crypto isakmp key cisco address 200.1.1.2
SAO-PAULO(config)#access-list 100 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
SAO-PAULO(config)#
SAO-PAULO(config)#crypto ipsec transform-set MYSET esp-aes esp-sha-hmac
SAO-PAULO(config)#crypto map MYMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
SAO-PAULO(config-crypto-map)#set peer 200.1.1.2
SAO-PAULO(config-crypto-map)#set transform-set MYSET
SAO-PAULO(config-crypto-map)#match address 100
SAO-PAULO(config-crypto-map)#exit
SAO-PAULO(config)#
SAO-PAULO(config)#interface gi 0/0/1
SAO-PAULO(config-if)#crypto map MYMAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

VPN – SOLUÇÃO - EXPLICAÇÃO

```
SAO-PAULO(config)#crypto isakmp policy 10
SAO-PAULO(config-isakmp)#authentication pre-share
SAO-PAULO(config-isakmp)#encryption aes
SAO-PAULO(config-isakmp)#hash sha
SAO-PAULO(config-isakmp)#group 2
SAO-PAULO(config-isakmp)#exit
```

Define a política e coloca um identificador nela

Define autenticação compartilhada

Define criptografia AES (Advanced Encrypt Standard)

Define o Hash SHA para garantir a integridade dos dados.

Define chave de 1024 bits e define Diffie – Hellman para intercâmbio da chave

VPN – SOLUÇÃO - EXPLICAÇÃO

```
SAO-PAULO(config)#crypto isakmp key cisco address 200.1.1.2
SAO-PAULO(config)#access-list 100 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
SAO-PAULO(config)#
SAO-PAULO(config)#crypto ipsec transform-set MYSET esp-aes esp-sha-hmac
```

Configura a chave pré-compartilhada usada na autenticação entre os roteadores. A senha é definida como cisco e o endereço IP do par remoto é 200.1.1.2

Lista de Acesso (Access List)

Cria um conjunto de transformação IPsec chamado MYSET, que define como os dados serão protegidos.

- esp-aes: Especifica AES como o algoritmo de criptografia.
- esp-sha-hmac: Define o HMAC SHA para autenticação e integridade dos dados.

O conjunto de transformação determina como os pacotes IPsec serão criptografados e autenticados na Fase 2.

VPN – SOLUÇÃO - EXPLICAÇÃO

```
SAO-PAULO(config)#crypto map MYMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
SAO-PAULO(config-crypto-map)#set peer 200.1.1.2
SAO-PAULO(config-crypto-map)#set transform-set MYSET
SAO-PAULO(config-crypto-map)#match address 100
SAO-PAULO(config-crypto-map)#exit
SAO-PAULO(config)#
SAO-PAULO(config)#interface gi 0/0/1
SAO-PAULO(config-if)#crypto map MYMAP
```

A crypto map é usada para associar o tráfego IPsec às interfaces.

Par Remoto

Associa ao conjunto definido anteriormente

Define a ACL que será utilizada

Aplica a **crypto map MYMAP** a essa interface. Isso ativa a VPN na interface e instrui o roteador a criptografar/descriptografar o tráfego com o par remoto conforme definido pela crypto map.

VPN – SOLUÇÃO – COMANDOS ÚTEIS

- **show crypto isakmp sa –** Verifica a Fase 1 (ISAKMP).
- **show crypto ipsec sa –** Verifica a Fase 2 (IPsec).
- **show crypto map –** Verifica as crypto maps aplicadas nas interfaces.
- **show crypto isakmp policy –** Confirma as políticas ISAKMP configuradas.
- **show crypto session –** Exibe um resumo dos túneis VPN.
- **show crypto engine connections active –** Mostra o tráfego criptografado.

3.

AVALIAÇÃO FINAL

Usando packet tracer

OBRIGADO!