REDES

AULA 4

Continuação sobre dispositivos de rede - PPT e Cisco

Acess Point (AP)

O Acess Point permite a conexão de dispositivos sem fio à rede cabeada, funcionando como um “extensor” do sinal.

Funções principais:

* Ampliação da cobertura Wi-Fi
* Autenticação e controle de acesso.
* Suporte a múltiplas SSIDs e VLANs

Gateway

O Gateway é um dispositivo (hardware ou software) que interliga redes diferentes, permitindo a comunicação entre sistemas que usam diferentes protocolos

Funções principais:

* Conversão de endereços e protocolos.
* Encaminhamento de tráfego entre redes.
* Implementação de regras de segurança.

Firewall

O firewall protege a rede bloqueando ou permitindo tráfego com base em regras de segurança.

Funções principais:

* Filtragem de pacotes
* Bloqueio de acessos não autorizados.
* Monitoramento de tráfego e logs

Tipos de Firewall:

* Firewall de software: Instalado em sistemas operacionais (exemplo: Windows Defender, IPTables no Linux.)
* Firewall de hardware: Equipamentos dedicados que protegem redes corporativas.

Transceiver – Transceptor/Conversor

Os transceivers são dispositivos responsáveis pela conversão e transmissão de sinais ópticos ou elétricos em redes de comunicação. Eles são usados para conectar switches, roteadores e outros equipamentos de rede.

Formas de Roteamento

* Estático
  + Configurar cada rota manualmente
* Dinâmico
  + Rota automática

O que são Modelos de Redes?

- Modelos de redes server como uma estrutura conceitual para descrever como a comunicação ocorre entre dispositivos

- Dois modelos principais: Modelo OSI e Modelo TCP/IP

Modelo OSI: 7 camadas

Camada 1 - Física

A primeira camada OSI é a camada física. Voltando para o exemplo dos correios, a camada física compreenderia as estradas, ou seja, o caminho que os pacotes percorrem para chegar ao destino.

Mas qual é a função da camada física do modelo OSI? Nesta camada são especificados os **dispositivos, como hubs** e os meios de transmissão, como os cabos de rede.

Os dados são transmitidos por esses meios e processados na próxima camada.

Camada 2 - Enlace ou Ligação

Fazendo um paralelo com os correios, essa camada funciona como um fiscal. Ele observa se os pacotes têm algum defeito em sua formatação e controla o fluxo com que eles são enviados.

Entenda a seguir, quais são as principais funções da camada de enlace do modelo OSI.

Nesta camada, os dados recebidos do meio físico são verificados para ver se possuem algum erro e, caso possuam, ele pode ser corrigido.

Dessa forma, as camadas superiores podem assumir uma transmissão praticamente sem erros. Esta camada também controla o fluxo que os dados são transmitidos.

É nela que são definidas as **tecnologias como as VLans**, ou **topologias** como a Token ring, ou a ponto-a-ponto.

Também é nela que **dispositivos como os switches** funcionam.

Esta camada é dividida em duas subcamadas: **A camada MAC e a camada LLC.**

**A subcamada MAC**

É esta camada que possibilita a conexão de diversos computadores em uma rede. Cada máquina conectada na rede tem um endereço físico, conhecido como **endereço MAC**.

É esse endereço que a camada utiliza para identificar e enviar os pacotes. Essa camada atua como uma interface entre a camada física e a subcamada LLC.

**A subcamada LLC**

É nesta camada que temos o controle de fluxo dos dados na rede. É por conta dela que conseguimos ter vários protocolos da próxima camada convivendo dentro de uma mesma rede.

Camada 3 - Rede

Quando estamos enviando uma carta, os correios verificam quem é o destinatário ou destinatária e quem é o (a) remetente da mensagem.

Se existirem muitas mensagens para serem enviadas, eles podem priorizar quais serão enviadas primeiro e qual é o melhor caminho para enviar essa carta.

Então, quais são os serviços oferecidos pela camada de rede do modelo OSI? Isso é justamente o que a camada três faz, ela atua como uma central dos correios.

Esta é talvez a camada mais atuante nas redes, principalmente na internet.

É nela que temos o endereçamento IP de origem e de destino; ela também pode priorizar alguns pacotes e decidir qual caminho seguir para enviar seus dados.

Essa camada, basicamente, controla o roteamento entre a origem e o destino do pacote.

*"Mas por que utilizar o endereço IP se já temos o endereço MAC?”*

**O endereço MAC** é o endereço físico de quem envia o pacote. Ou seja, se enviarmos um pacote e ele passar por cinco dispositivos diferentes (roteadores, switches, ou servidores, por exemplo) o endereço MAC é alterado no processo. Já o endereço IP não sofre essa alteração.

**O endereço IP** é a identificação da sua máquina na rede. É aquele endereço como 192.168.0.1.

É nessa camada que temos protocolos como o **IP** ou o **ICMP**. Bem, as cartas chegaram à central dos correios, agora elas precisam ser transportadas.

Camada 4 - Transporte

Se na camada um temos as estradas e os caminhos que os dados percorrem, na camada quatro temos os caminhões e os carteiros ou carteiras.

É esta camada que garante o envio e o recebimento dos pacotes vindos da camada três. Ela gerencia o transporte dos pacotes para garantir o sucesso no envio e no recebimento de dados.

Esta camada lida muito com a qualidade do serviço para que os dados sejam entregues com consistência, isto é, sem erros ou duplicações. Porém, nem todos os protocolos desta camada garantem a entrega da mensagem.

Protocolos muito comuns dessa camada são os protocolos **TCP** em **UDP**.

O primeiro garante a entrega da mensagem, diferente do segundo. Por não garantir a entrega da mensagem, o protocolo UDP é um pouco mais rápido que o TCP.

Bem, mas para ocorrer o transporte de um pacote entre os computadores, é necessário que as máquinas consigam se comunicar. Isso é função da próxima camada.

Leia também: O que é UDP e TCP? Entenda quais as diferenças e como funciona cada Protocolo

Camada 5 - Sessão

Esta camada é responsável por estabelecer e encerrar a conexão entre hosts. É ela quem inicia e sincroniza os hosts.

Além de realizar o estabelecimento das sessões, esta camada também provém algum suporte a elas, como registros de log e realização de tarefas de segurança.

Recebemos os pacotes, vamos checá-los para ver que dados têm dentro? Ainda não podemos.

Os dados ainda precisam ser tratados para serem usados. Como a camada de sessão só é responsável por estabelecer a conexão entre os hosts, o tratamento dos dados é de responsabilidade da próxima camada.

Camada 6 - Apresentação

Esta é a camada responsável por fazer a tradução dos dados para que a próxima camada os use.

Nesta camada temos a conversão de códigos para caracteres, a conversão e compactação dos dados, além da criptografia desses dados, caso necessite.

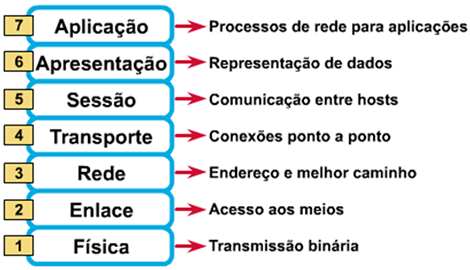
Depois de tratados, esses dados estão prontos para serem usados na próxima camada.

Camada 7 - Aplicação

**A última camada do modelo OSI é a camada para consumir os dados.** Nesta camada, temos os programas que garantem a interação humano-máquina.

Mas, qual é a função da camada de aplicação? Nela conseguimos enviar e-mails, transferir arquivos, acessar websites, **conectar remotamente em outras máquinas**, entre outras coisas (Falando em conectar remotamente, você conhece as diferenças entre Telnet e SSH?).

É nesta camada que temos os protocolos mais conhecidos como o **HTTP, FTP, além de serviços como o DNS**.



TCP/IP

* As Camadas 1 e 2 do modelo OSI estão agregadas na camada 1 do TCP/IP ou Acesso aos Meios.
* A Camada 3 do modelo OSI (Redes) é chamada de Internet no TCP/IP.
* A Camada 4 tanto no modelo OSI como no TCP/IP são chamadas de camada de Transporte.
* As Camadas 5, 6 e 7 do modelo OSI são agregadas em uma só camada no TCP/IP, a qual é chamada de camada de Aplicação.

IPv4 e IPv6

O Que é IP?

Endereço IP é um endereço exclusivo que identifica um dispositivo na Internet ou em uma rede local. IP vem do inglês "Internet Protocol" (protocolo de rede) que consiste em um conjunto de regras que regem o formato de dados enviados pela Internet ou por uma rede local.

**O que é Endereço IPv4?**

O endereço IPv4, também conhecido como Protocolo de Internet versão 4, é um sistema de endereçamento numérico utilizado para identificar e localizar dispositivos conectados em uma rede de computadores. Ele é composto por uma sequência de 32 bits, dividida em quatro grupos de oito bits cada, separados por pontos. Cada grupo pode variar de 0 a 255, o que resulta em um total de aproximadamente 4,3 bilhões de endereços IPv4 possíveis.

**Como funciona o Endereço IPv4?**

O endereço IPv4 é utilizado para identificar de forma única cada dispositivo conectado a uma rede. Ele é composto por duas partes principais: a identificação da rede e a identificação do host. A identificação da rede é responsável por indicar qual rede o dispositivo está conectado, enquanto a identificação do host identifica o dispositivo específico dentro dessa rede.

Para entender melhor como funciona o endereço IPv4, é importante conhecer alguns conceitos básicos. O endereço IP é dividido em classes, que determinam a quantidade de bits utilizados para a identificação da rede e do host. As classes mais comuns são a Classe A, Classe B e Classe C.

**Classes do Endereço IPv4**

A Classe A é utilizada para redes de grande porte, como empresas e provedores de internet. Nessa classe, o primeiro octeto (grupo de oito bits) é utilizado para identificar a rede, enquanto os três octetos restantes são utilizados para identificar o host. Isso permite que a Classe A suporte um grande número de dispositivos em uma única rede.

A Classe B é utilizada para redes de médio porte, como universidades e empresas de médio porte. Nessa classe, os dois primeiros octetos são utilizados para identificar a rede, enquanto os dois octetos restantes são utilizados para identificar o host. Isso permite que a Classe B suporte um número intermediário de dispositivos em uma única rede.

A Classe C é utilizada para redes de pequeno porte, como residências e pequenas empresas. Nessa classe, os três primeiros octetos são utilizados para identificar a rede, enquanto o último octeto é utilizado para identificar o host. Isso permite que a Classe C suporte um número limitado de dispositivos em uma única rede.

**O que é Endereço IPv6?**

O endereço IPv6, também conhecido como Protocolo de Internet versão 6, é um sistema de endereçamento utilizado para identificar e localizar dispositivos conectados à internet. Ele é a versão mais recente do protocolo de internet e foi desenvolvido para substituir o IPv4, que está se esgotando devido ao crescimento exponencial da internet e ao aumento do número de dispositivos conectados. O IPv6 foi projetado para fornecer um número muito maior de endereços IP disponíveis, além de oferecer melhorias em termos de segurança, eficiência e escalabilidade.

**Por que o IPv6 é necessário?**

Com o rápido crescimento da internet e a proliferação de dispositivos conectados, o IPv4, que é baseado em um sistema de endereçamento de 32 bits, está se aproximando de sua capacidade máxima. Isso significa que em breve não haverá mais endereços IPv4 disponíveis para alocar a novos dispositivos. O IPv6, por outro lado, utiliza um sistema de endereçamento de 128 bits, o que permite um número praticamente ilimitado de endereços IP. Além disso, o IPv6 oferece melhorias em relação ao IPv4, como maior segurança, melhor desempenho e suporte nativo para recursos como mobilidade e qualidade de serviço.

**Como funciona o endereço IPv6?**

O endereço IPv6 é composto por 8 grupos de 4 dígitos hexadecimais separados por dois pontos. Cada dígito hexadecimal representa 4 bits, o que resulta em um total de 128 bits para o endereço IPv6. Essa representação em hexadecimal permite uma maior variedade de combinações e facilita a leitura e escrita dos endereços. Além disso, o IPv6 utiliza uma estrutura hierárquica, onde os primeiros bits do endereço identificam a rede e os últimos bits identificam o dispositivo específico dentro da rede. Isso permite uma melhor organização e gerenciamento dos endereços IP.

Exemplo de endereço IPv4 em binário:

192 – 110000 -> 128|64|32|16|8|4|2|1

168 – 10101000 -> 128|64|32|16|8|4|2|1

1 – 00000001 -> 128|64|32|16|8|4|2|1

12 – 00001100 -> 128|64|32|16|8|4|2|1

0 = Não cabe (128 não cabe em 1), 1 = Cabe (1 cabe em 1)

Clique na imagem para uma versão maior

Nome:          binario-9.jpg
Visualizações: 4013
Tamanho:  160,9 KB
ID:       41598

Exercícios de conversão de IP:

1. 172.16.0.194
2. 10.108.200.33
3. 192.169.253.45
4. 35.215.58.98
5. 173.255.227.4

128|64|32|16|8|4|2|1

A – 10101100 . 00010000 . 00000000 . 11000010

B – 00001010 . 01101100 . 11001000 . 00100001

C – 11000000 . 10101001 . 11111101 . 00101101

D – 00100011 . 11010111 . 00111010 . 01100010

E – 10101101 . 11111111 . 11100011 . 00000100

As classes de endereço mais utilizadas são as classes A, B e C.

Endereços especiais (Empresas):

|  |  |  |
| --- | --- | --- |
| LAN Private Class A  LAN Private Class B  LAN Private Class C | 10.0.0.0/8  172.16.0.0/12  192.168.0.0/16 | 10.255.255.255  172.31.255.255  192.168.255.255 |

Endereços especiais:

|  |  |  |
| --- | --- | --- |
| Multicast Class D | 224.0.0.0/4 | 239.255.255.255 |
| Local Host “loopback” | 127.0.0.0/8 | 127.255.255.255 |

Máscaras de Sub-rede

Uma máscara de sub-rede é usada para dividir uma rede IP em sub-redes menores, o que facilita a organização e o gerenciamento da rede. Ela define qual parte do endereço IP é a parte da rede e qual parte é a parte do host. A notação CIDR (Classless Inter- Domain Routing) é uma maneira de representar a máscara de sub-rede, como /24, que indica que os primeiros 24 bits do endereço IP são usados para a rede.

Rede Original: 192.168.1.0/24

•Endereço IP: 192.168.1.0

•Máscara de sub-rede: 255.255.255.0 (ou /24)

•Número de endereços na rede: 2^(32-24) = 2^8 = 256

•Endereços disponíveis para hosts: 256 - 2 (rede e broadcast) = 254

/x -> Usado para determinar a rede, separa bits para a rede

/24 -> separa os 3 primeiros octetos para a rede, congela esses octetos

/16 -> Congela 16 bits, ou seja, os 2 primeiros octetos

/8 -> Congela 8 bits, ou seja, apenas o primeiro octeto

Exemplo

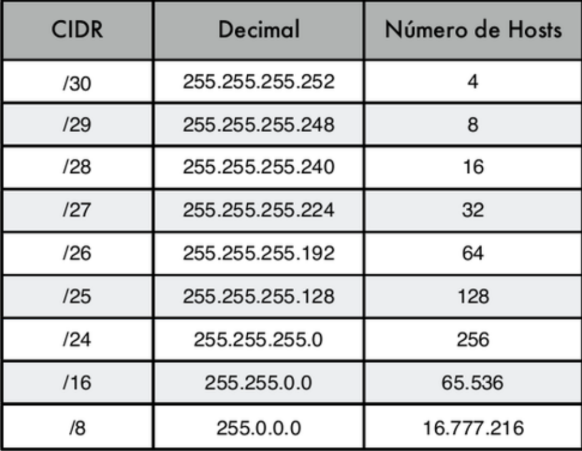
10.108.1.33 /24 (Definiu a rede – 10.108.1)

10.108.1.34 (Mesma rede)

10.108.1.240 (Mesma rede)

10.108.11.35 (Rede diferente, o penúltimo octeto não é igual)

Se fosse /16, todos seriam da mesma rede, os bits que não foram reservados para rede, são reservados para o host, portanto, podem mudar. Os bits reservados para a rede não podem mudar, eles congelam.



Todos esses são endereços de IP utilizados por hosts.

Um endereço de rede é calculado:

Ex:

IP Host: 10.108.1.33

O IP de rede é calculado usando o IP do Host e a máscara, se 0 + 1, então = 0, se 1 + 1, então = 1 e se 0 + 0 = 0. Por isso, os primeiros 24 bits ficam iguais ao do IP do Host.

00001010.01101100.00000001.00100001

Máscara: 255.255.255.0 (/24)

11111111.11111111.11111111.00000000

IP de Rede: 10.108.1.0 /24

00001010.01101100.00000001.00000000

Endereço de Broadcast: 10.108.1.255

00001010.01101100.00000001.11111111

O último octeto do endereço de Broadcast é o inverso do último octeto do IP de rede.

Ex:

IP de host: 00001010.01101100.00000001.11000000 (10.108.1.192)

Máscara: 11111111.11111111.111111111.110000000 /26

IP de Rede: 00001010.01101100.00000001.11000000

IP de Broadcast: 00001010.01101100.00000001.00111111

Exercício:

Mostrar endereços de rede de 3 redes diferentes (Endereço base: 10.108.200.??? /X)

Rede ADM – 16:

IP de Host: 10.108.200.1

00001010.01101100.11001000.00000001

Máscara: 255.255.255.240 /28 (16 hosts)

11111111.11111111.11111111.11110000

IP de Rede: 10.108.200.0

00001010.01101100.11001000.00000000

Rede Impressoras – 8:

IP de Host: 10.108.200.17

00001010.01101100.11001000.00010001

Máscara: 255.255.255.248 /29 (8 hosts)

11111111.11111111.11111111.11111000

IP de Rede: 10.108.200.16

00001010.01101100.11001000.00010000

Restante – 232:

IP de Host: 10.108.200.33

00001010.01101100.11001000.00100001

Máscara: 255.255.255.0 /24 (256 hosts – Comporta os 232)

11111111.11111111.11111111.00000000

IP de Rede: 10.108.200.0

00001010.01101100.11001000.00000000

(Exercícios realizados desconsiderando a retirada de 2 endereços reservados para Rede e Broadcast)

Atividade:

Para cada endereço IP e máscara, identifique:

1. O endereço da rede.
2. O primeiro IP válido para o host.
3. O último IP válido para rede.
4. O endereço de broadcast.

IP: 192.168.1.25 /24:

Máscara: 255.255.255.0

IP da Rede: 192.168.1.0

Primeiro válido: 192.168.1.1

Último válido: 192.168.1.254

IP de Broadcast: 192.168.1.255

IP: 10.0.5.200 /8:

Máscara: 255.0.0.0

IP da Rede: 10.0.0.0

Primeiro válido: 10.0.0.1

Último válido: 10.255.255.254

IP de Broadcast: 10.255.255.255

IP: 172.20.35.180 /16:

Máscara: 255.255.0.0

IP da Rede: 172.20.0.0

Primeiro válido: 172.20.0.1

Último válido: 172.20.255.254

IP de Broadcast: 172.20.255.255

IP: 192.168.15.240 /24:

Máscara: 255.255.255.0

IP da Rede: 192.168.15.0

Primeiro válido: 192.168.15.1

Último válido: 192.168.15.254

IP de Broadcast: 192.168.15.255

IP: 10.10.8.145 /8:

Máscara: 255.0.0.0

IP da Rede: 10.0.0.0

Primeiro válido: 10.0.0.1

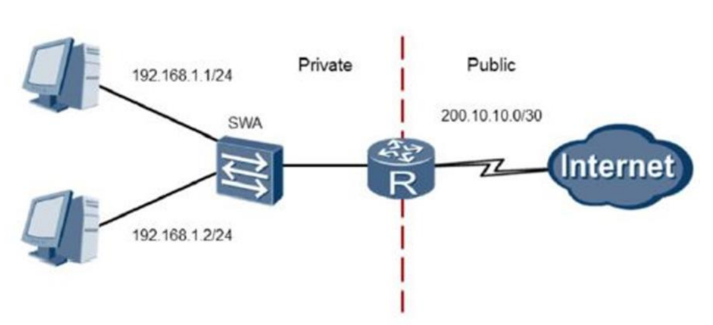
Último válido: 10.255.255.254

IP de Broadcast: 10.255.255.255

NAT (Network Address Translation)

Técnica que permite a um conjunto de endereços IP privados serem mapeados para um endereço IP público, ajudando a economizar endereços IPv4.

Ele permite que excedamos o limite de endereços IPv4 (Lembrando que não haveriam endereços suficientes para todos), logo, ele permite que todos continuem usando o IPv4



NAT Estático, NAT Dinâmico e PAT (Port Address Translation)

NAT Estático é um tipo de tradução de endereços de rede onde um endereço IP privado é mapeado para um endereço IP público de forma fixa e permanente. Esse mapeamento é configurado manualmente pelo administrador da rede.

NAT Dinâmico, também conhecido como NAT Overload, é um tipo de tradução de endereços de rede onde múltiplos endereços IP privados são mapeados para um conjunto de endereços IP públicos de forma dinâmica.

PAT, também conhecido como NAT Overloading, é um tipo de tradução de endereços de rede onde múltiplos endereços IP privados compartilham um único endereço IP público, utilizando diferentes números de portas TCP ou UDP.

CGNAT (Carrier-Grade Network Address Translation) – “NAT dentro do NAT”

CGNAT (Carrier-Grade Network Address Translation) é uma técnica utilizada por provedores de serviços de Internet, como a CLARO, (ISPs) para gerenciar a escassez de endereços IPv4 públicos. CGNAT permite que múltiplos clientes compartilhem um único endereço IPv4 público, utilizando NAT (Network Address Translation) em uma escala muito maior do que a tradicionalmente utilizada em redes domésticas ou corporativas.

