

SERVIDORES E SERVIÇOS DE INTERCONNECTIVIDADE WINDOWS

UNIDADE 4 – CONHECENDO O PROTOCOLO IP, AS FORMAS DE CONFIGURAÇÃO E OS MÉTODOS DE GERENCIAMENTO

Autor: Denilson Bonati

Revisora: Cilene Renata Real

INICIAR

Introdução

Nesta unidade, conheceremos as formas como devemos proceder para realizar o endereçamento IP de pequenas e grandes infraestruturas. Como este procedimento pode ser realizado manualmente ou com recursos automáticos de entrega de endereços, saberemos como gerenciar essas entregas e quais ferramentas podem ser utilizadas para isso. Conheceremos quais são as aplicabilidades das duas formas: estática e automática.

Outro recurso importante que será estudado nesta unidade chama-se IIS, serviço da Microsoft para servidores web. Estudaremos como podemos utilizar o servidor para hospedar sites que poderão estar disponíveis na intranet da empresa ou até mesmo para toda a internet. Por fim, conheceremos a ferramenta IPAM (gerenciamento de endereço IP) e qual sua função dentro de uma estrutura em que a entrega de IPs é feita de modo automático.

4.1 Endereçamento IP

Para que computadores, smartphones, videogames, televisores e outros dispositivos pertencentes a uma rede possam trocar informações, eles precisam ser identificados e localizados. Para isso, é utilizado um protocolo específico, presente na pilha de protocolos utilizados em uma rede: o protocolo IP (*Internet protocol* – em português, protocolo de internet). Vale lembrar que, mesmo que um equipamento possua um nome como Servidor1, por exemplo, ele sempre será identificado e localizado pelo seu endereçamento IP, cabendo ao

servidor DNS realizar a tradução do nome do equipamento para o seu endereçamento IP. Atualmente, duas versões do IP estão em uso, o Ipv4 e o Ipv6. Dentre elas, o primeiro ainda é predominante. Essa versão possui um endereçamento composto de um número de 32 BIT. Com isso, é possível criar 4.294.967.296 bilhões de combinações diferentes de endereçamento. O número parece extenso, mas os endereçamentos Ipv4 estão se esgotando e, em algumas regiões do mundo, já se esgotaram, principalmente pela alta demanda de novos dispositivos e sites presentes na internet. Por conta disso, seu sucessor natural, o Ipv6, já está em uso, funcionando provisoriamente em conjunto com o Ipv4. O Ipv6 funciona com um endereçamento de 126 BIT, o que garante 340 undecilhões de endereços. Como a grande maioria das redes locais e ainda a maior parte da internet utiliza o IPv4, iremos focar em sua utilização.

O endereçamento IPv4 é dividido em quatro números, separados por pontos. Esses números são chamados de octetos, pois são formados por oito bits, cada um. Por exemplo, o IP 192.168.1.101 pode ser convertido para binário, gerando o número 11000000.10101000.00000001.01100101.



VOCÊ SABIA?

Em caso de dúvida sobre como realizar a conversão de binário em números decimais ou, ainda, se for necessário rever os conceitos de rede e sub-rede, acesse o link abaixo:< <http://deptal.estgp.pt:9090/cisco/ccna1/course/module8/8.1.1.3/8.1.1.3.html>>

Duas versões do IP estão atualmente em uso: a v4 e a v6. Por enquanto, a v4 ainda domina [...] mas o uso da v6 está aumentando. Cada pacote v4 inicia com um cabeçalho de 40 bytes contendo um endereço de origem de 32 bits e um endereço de destino de 32 bits, entre outros campos. Esses campos são chamados de endereços IP e formam a base do roteamento na Internet. Eles são convencionalmente escritos como quatro conjuntos de números decimais na faixa de 0-255 separados por pontos, como 192.31.231.65 (TANENBAUM, 2016, p. 365).

O Ipv4 está dividido em cinco classes distintas, nomeadas de A até E. Sobre isso, falaremos abaixo.

Cinco classes do Ipv4

» Clique nas abas para saber mais sobre o assunto

Classe A	Classe B	Classe C	Classe D	Classe E
----------	----------	----------	----------	----------

A Tabela 1 ilustra as classes de rede que podem ser utilizadas no Ipv4, com suas respectivas quantidades de redes e computadores.

Tabela 1 – Tabela comparativa de classes utilizadas no endereçamento Ipv4

Classe	Abrangência do primeiro byte	Número de redes	Computador por rede	Máscara de sub-rede padrão
A	001 - 126	126	16.777.214	255.0.0.0
B	128 -191	16.384	65.534	255.255.0.0
C	192 - 223	2.097.150	254	255.255.255.0
D	224 - 239	-	-	-
E	240 - 255	-	-	-

Fonte: SERAGGI, 2019, p. 41.

Observe que a Tabela 1 apresenta a máscara de sub-rede padrão utilizada em cada classe de rede. Vamos entender qual é sua função.

4.1.1 Máscaras de rede

O endereçamento IP não identifica apenas um host da rede, mas também a rede à qual o host pertence. Esta informação é fornecida em outro número de 32 bits, chamado máscara de sub-rede. Por padrão, a máscara de sub-rede de um endereçamento IP de classe C é 255.255.255.0, indicando que os três primeiros octetos indicam a rede, e o último octeto, o número do host da rede (computadores, celulares etc). Em binário, o valor decimal 255.255.255.0 é lido como 11111111.11111111.11111111.0.

Suponhamos que um determinado computador receba o IP de classe C 192.168.100.10, com a máscara de sub-rede indicada como 255.255.255.0. Sabemos, então, que o computador será indicado pelo número 10 e sua rede é 192.168.100. Por padrão, este computador somente poderá se comunicar com outros hosts pertencentes à mesma rede 192.168.100.

É possível configurar o endereço IP de um host, a sua máscara de sub-rede e outras informações importantes, como os servidores DNS e o endereço IP do gateway de acesso a outra rede, manualmente. Para uma grande quantidade de dispositivos em uma rede, é aconselhável o preenchimento automático dessas informações, através de um serviço chamado de DHCP (*Dynamic Host Configuration Protocol* – em português, Protocolo de configuração dinâmica de host)

4.1.2 Estático

O endereço estático, também chamado de endereço fixo, normalmente é preenchido de modo manual pelo administrador da rede. Esse endereço irá permanecer fixo, ou seja, o host sempre terá o mesmo endereçamento IP em uma rede. A configuração estática de endereçamento IP normalmente é realizada em hosts que precisam ser identificados por seus IPs. Por isso, não pode haver uma alteração neste endereçamento, o que ocasionaria problemas em máquinas clientes dependentes de serviços e funções desses computadores ou dispositivos. A configuração estática de IP normalmente é aplicada a servidores e outros dispositivos importantes para o funcionamento de uma rede, como roteadores. A configuração de um IP fixo para o servidor pode ser realizada pelo painel Local Server, na janela do Server Manager, no item Ethernet. Em máquinas clientes da rede, como o sistema operacional Windows, essa configuração pode ser realizada no painel de controle nas configurações de rede e internet.

É importante observar, na definição do endereçamento IP, a versão do protocolo que deverá ser utilizada. A Figura 1 demonstra a escolha de configuração do endereçamento IP na versão 4.

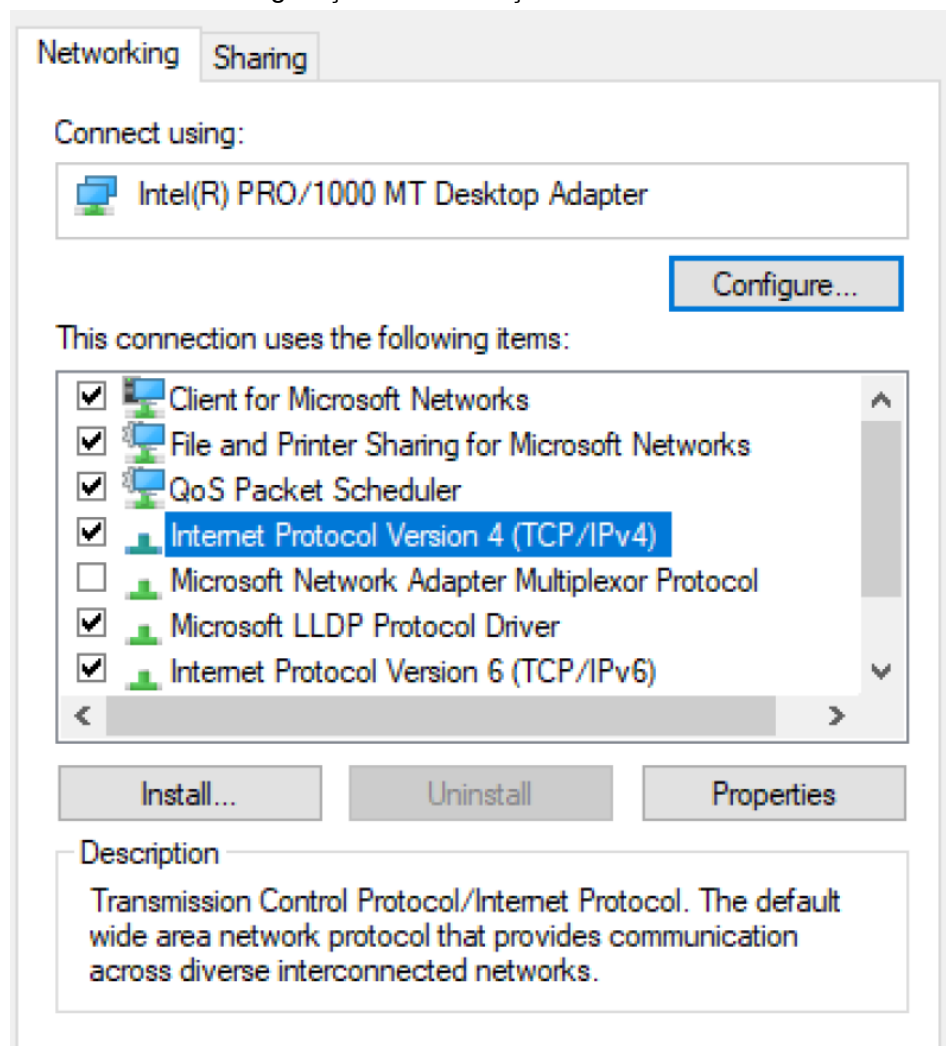


Figura 1 – Escolha da versão do protocolo a ser configurado.

Observe, pela Figura 2, que é necessário definir a forma como o IP será configurado. Na opção **Obtain an IP address automatically** (Obter um endereço IP automaticamente), em que o dispositivo irá aguardar a entrega de um IP via servidor DHCP, ou **Use the following ip address** (Use o seguinte endereço IP), na qual o endereçamento deve ser feito manualmente, o dispositivo receberá um IP estático.

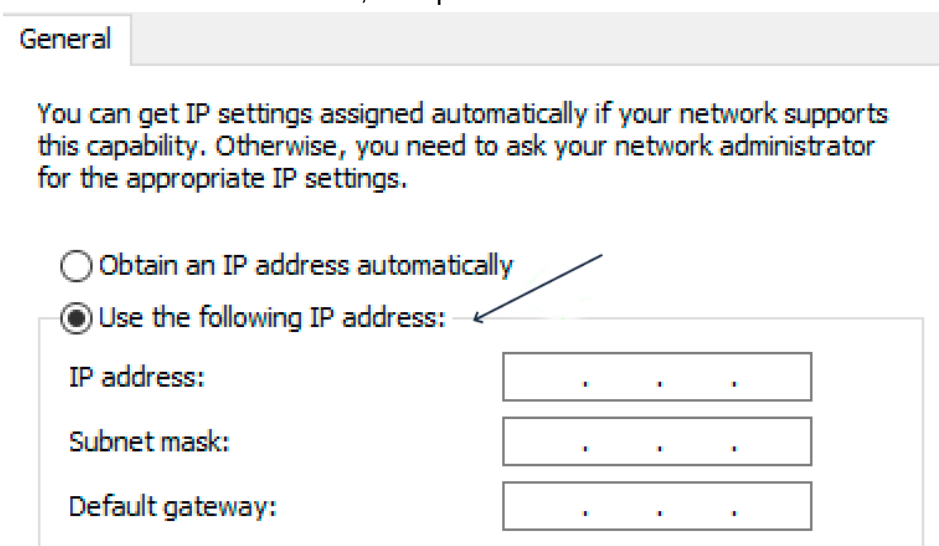


Figura 2 – Definição de IP estático.

Veja, na Figura 3, que as seguintes configurações deverão ser indicadas: IP address (endereçamento IP) – Endereço IP fixo que o host irá possuir; Subnet mask (máscara de sub-rede) – Máscara a ser utilizada no endereçamento. Neste exemplo, foi utilizada a máscara padrão 255.255.255.0; Default gateway (Gateway padrão) – O endereço do gateway padrão, é o endereço IP do dispositivo de rede, normalmente um roteador que dará acesso a este host de outra rede. Caso este host tenha acesso à internet, é necessário indicar o endereço IP do roteador que dará acesso a outra rede, fora da rede local – neste exemplo, a internet.

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192 . 168 . 100 . 50

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 100 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 100 . 10

Alternate DNS server: 8 . 8 . 8 . 8

☐ Validate settings upon exit

Advanced...

Figura 3 – Configurações de IP, máscara de sub-rede e DNS.

Ainda na Figura 4 é apresentada a configuração de DNS. Neste caso, especificando manualmente os endereços IPs dos servidores de DNS primário, ou seja, o servidor DNS da rede local, o mesmo servidor pode acumular o serviço de controlador de domínio (AD DS) e o servidor de DNS alternativo ou secundário, que será o responsável pela resolução de nomes em IPs da rede externa – no caso, a internet. Na configuração do servidor secundário, o IP de um servidor de DNS público pode ser utilizado, como no exemplo do servidor de DNS público do Google, com o endereço IP 8.8.8.8. É importante saber que, em caso de alguma alteração ser necessária, toda a configuração deve ser feita manualmente. Em casos de uma rede com uma grande quantidade de hosts, a configuração manual de endereços IPs pode ser um procedimento muito trabalhoso para o administrador.

4.1.3 Dinâmico

Acredito que você deva possuir uma rede Wi-fi em sua residência ou local de trabalho. Normalmente, quando algum convidado frequenta sua casa ou trabalho, é muito comum ouvir deste convidado: “Qual a senha do Wi-

fi?” Provavelmente você nunca ouviu “Qual a faixa de IP de sua rede local, para que eu acesse a internet?”. Isso ocorre porque, para o convidado para ter acesso à internet, o seu dispositivo ou computador recebe um endereçamento IP com as configurações de sub-rede e DNS automaticamente. Este procedimento é feito, na maioria dos casos, em uma rede doméstica, pelo roteador. É inviável que a configuração de endereçamento IP seja feita manualmente, principalmente em redes Wi-fi. O usuário convencional não terá conhecimento técnico para isso, sem falar que as configurações manuais, além de serem mais demoradas, podem apresentar falhas, como a configuração de endereçamento IPs iguais em uma rede, ocasionando conflito.

Para facilitar a configuração IP, não só em redes Wi-fi, mas também em redes cabeadas de médias e grandes infraestruturas, a entrega de IPs automaticamente pode ser um recurso extremamente útil para o administrador da rede.

Em uma rede pequena, com poucos equipamentos, seria fácil inserir manualmente os números de IP dos computadores, mas em uma rede com 150 computadores, 5 impressoras a laser, 2 servidores NAS, 10 roteadores e mais alguns equipamentos de rede, ficaria mais difícil. Por isso, a instalação e configuração correta do DHCP é de suma importância para o bom funcionamento do servidor e da rede (SERAGGI,2019, p. 184).

Este serviço, como já dito, pode ser realizado por um roteador ou, em infraestruturas nas quais este serviço deva ser mais controlado, pode-se utilizar o serviço de DHCP do Windows Server. Dessa forma, os IPs de todos os clientes da rede serão entregues pelo servidor e será possível controlar e renovar IPs de uma maneira mais personalizada, que atenda às demandas da infraestrutura.

4.1.4. Instalando e configurando um servidor DHCP

O serviço de DHCP pode ser instalado no Windows Server 2019 pelo Assistente **Add Roles and Features**, presente no Server Manager.

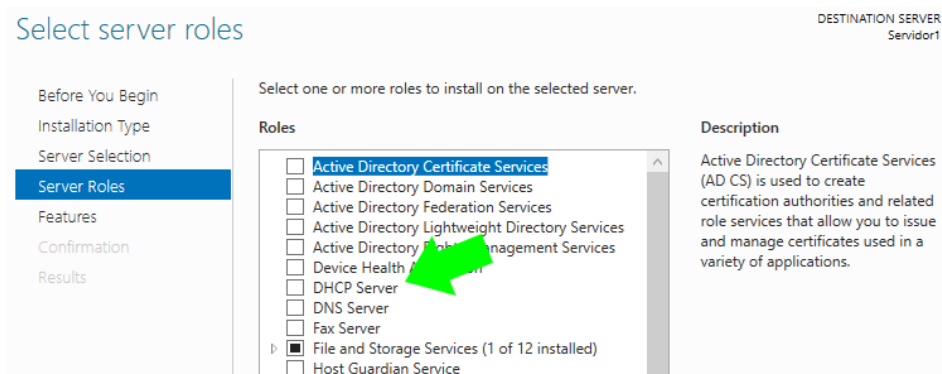
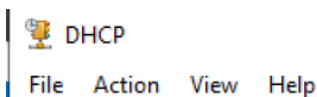


Figura 4 – Instalação do Serviço DHCP em um servidor com Windows Server 2019.

Após a instalação dos recursos, o serviço DHCP pode ser acessado pelo menu **Tool**, presente no Server Manager, selecionando a opção DHCP.

O serviço DHCP pode entregar IPs nas versões 4 e 6. Neste exemplo, iremos configurar o serviço de entrega para Ipv4.



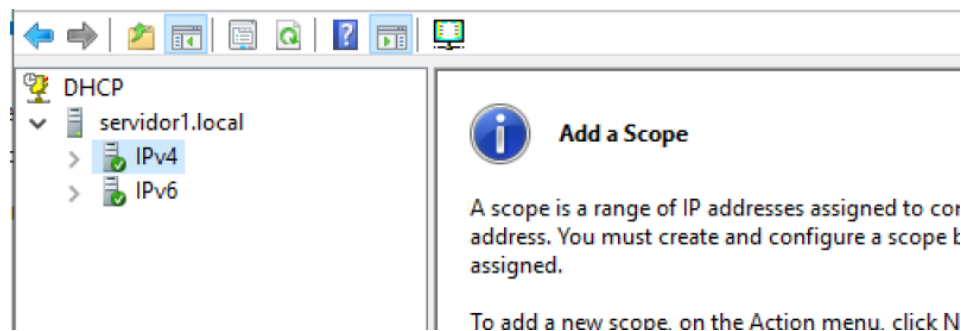


Figura 5 – Janela de configuração do serviço DHCP.

A configuração de entrega de IPs é feita através de escopos. Um escopo é uma configuração de intervalos de IPs que serão entregues. Clicando sobre o Ipv4, com o botão da direita, é possível selecionar a opção **New Scope** (Novo Escopo). A primeira tarefa a ser feita é indicar um nome e uma descrição para o escopo, caso seja necessário.

Scope Name
You have to provide an identifying scope name. You also have the option of providing a description.

Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name: Rede Local

Description: Entrega de IPs para a rede local

Figura 6 – Criação de um novo escopo de entrega de IPs.

Avançando no assistente, o próximo passo é configurar o escopo. Neste exemplo, o serviço de DHCP irá entregar os IPs para a rede 192.168.100.0/24, ou seja, a máscara aplicada será a máscara padrão 255.255.255.0. O IP inicial para a entrega será o IP 192.168.100.50. É importante deixar uma faixa de IPs disponível para computadores e dispositivos que necessitam de endereçamentos IP fixo, como servidores, por exemplo. Neste exemplo, a faixa do IP inicial 192.168.100.1 até 192.168.100.49 será reservada para os servidores e demais equipamentos de rede que necessitam de IPs fixos.

É necessário, também, indicar o último IP que será entregue pelo escopo – neste exemplo, o IP 192.168.100.254.

A máscara a ser aplicada ao IP também deve ser indicada na configuração.

IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 100 . 50

End IP address: 192 . 168 . 100 . 254

Configuration settings that propagate to DHCP Client

Length: 24

Subnet mask: 255 . 255 . 255 . 0

Figura 7 – Configuração da faixa de entrega de IPs do escopo.

Avançando no assistente de configuração, é possível definir exclusões de entrega dentro do escopo criado. Sabendo que o escopo entregará os IPs de 192.168.100.50 até 192.168.100.254, pode-se definir que os endereços de 192.168.100.100 até 192.168.100.130 não serão entregues pelo escopo. Desse modo, também é possível deixar esta faixa para outros equipamentos e computadores que necessitem de IPs fixos. Esse procedimento não é obrigatório, podendo ser deixado em branco, caso não sejam necessárias exclusões dentro do escopo.

Figura 8 – Definição de exclusão de entrega dentro do escopo.

O próximo passo é definir o período de concessão de IPs, ou seja, quando um computador ou dispositivo receber um IP via este escopo, definir por quanto tempo este endereçamento IP irá permanecer com o cliente, sem a necessidade de renovar a concessão. O padrão costuma ser de oito dias, mas este prazo pode ser diminuído ou alterado, dependendo da necessidade.

Figura 9 – Tempo de concessão de endereçamento IP.

A seguir, a próxima configuração é o IP do gateway da rede, que será entregue automaticamente pelo escopo. Neste exemplo, o IP indicado foi 192.168.100.1. Caso a rede não possua gateway, a configuração pode ser deixada em branco.

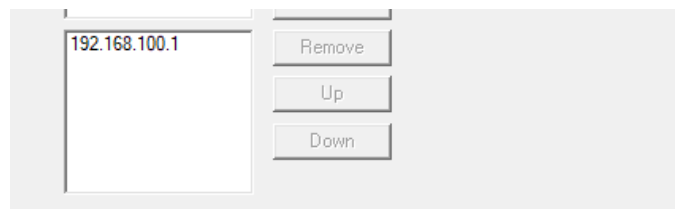


Figura 10 – Definição do gateway que será entregue pelo escopo.

O próximo passo é indicar os endereçamentos dos servidores DNS da rede.

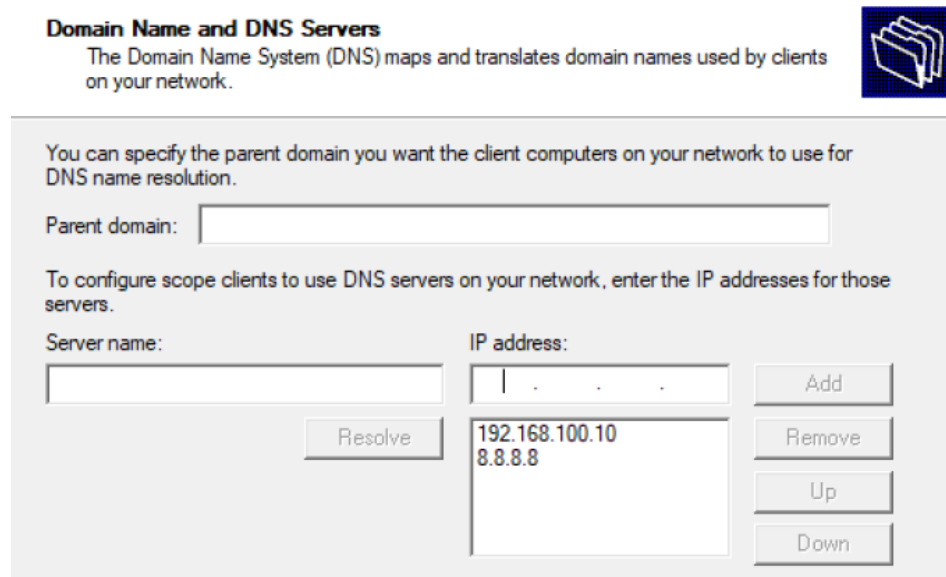


Figura 11 – Definição dos endereços IPs dos servidores DNS.

A seguir, é necessário definir se este escopo já estará ativo, ou seja, se o serviço de DHCP através deste escopo já estará entregando IPs ou estará inativo. Selecionando **Yes** (Sim) e clicando em **Finish**, o serviço DHCP estará ativo junto ao escopo.

Todo computador da rede 192.168.100.0 que estiver configurado para receber o IP automaticamente irá receber o IP deste escopo.

Uma forma de descobrir se a máquina cliente da rede recebeu o endereçamento IP é utilizar o prompt de comando e digitar o comando `ipconfig`.

```
C:\Users\user>ipconfig
Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::198:b1d0:c31c:e15%3
    IPv4 Address. . . . . : 192.168.100.50
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.100.1

Tunnel adapter isatap.{A9029DEB-49B4-49F5-A31C-86D54225110D}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\user>
```

Figura 12 – IP recebido pela máquina cliente da rede através do escopo recém-criado.

Observe que é possível visualizar o endereço IP recebido, além das configurações de Gateway.

4.2 IIS

Provavelmente, você já deve ter se perguntado onde os filmes do catálogo da Netflix estão salvos ou, ainda, onde estão salvos os arquivos do seu website preferido. Como esses arquivos de filmes, documentos HTML e imagens podem ser acessados via browser ou aplicativo? Todos esses arquivos estão salvos em servidores que estão disponíveis e acessíveis via protocolo HTTP ou outro protocolo adequado para vídeos ou demais arquivos de mídia.

O Windows Server possui um serviço de publicação e acesso a arquivos via intranet, ou seja, rede local, ou diretamente pela internet, caso o servidor esteja acessível e disponível via internet. Esse serviço é conhecido como IIS (Internet Information Services). A função do IIS no Windows Server é oferecer uma plataforma para a hospedagem de sites, serviços e aplicativos.

4.2.1 Instalando os recursos de servidor WEB (IIS)

Como toda instalação de serviços e recursos no Windows Server, a instalação IIS pode ser feita através do Assistente **Add Roles and Features**, presente no Server Manager.

A instalação pode ser feita no assistente, selecionando **Web Server IIS**.

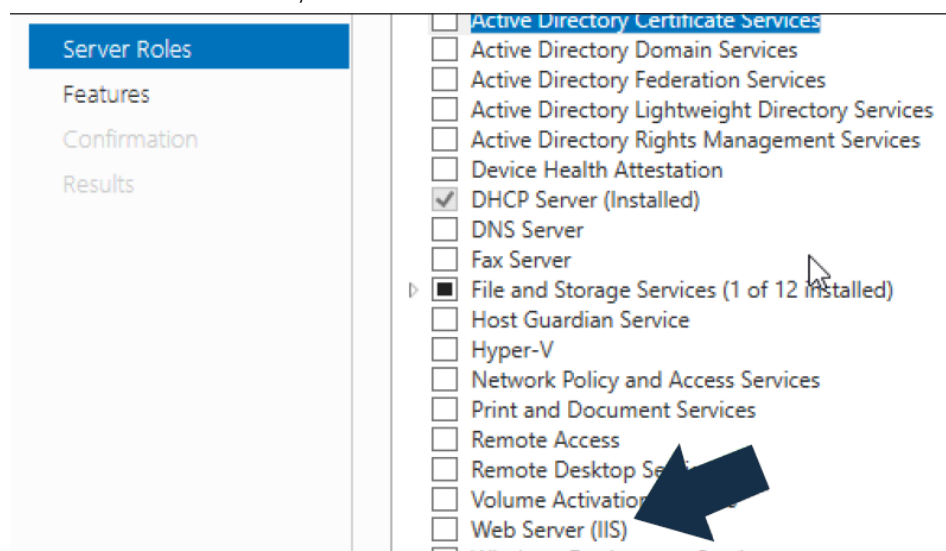
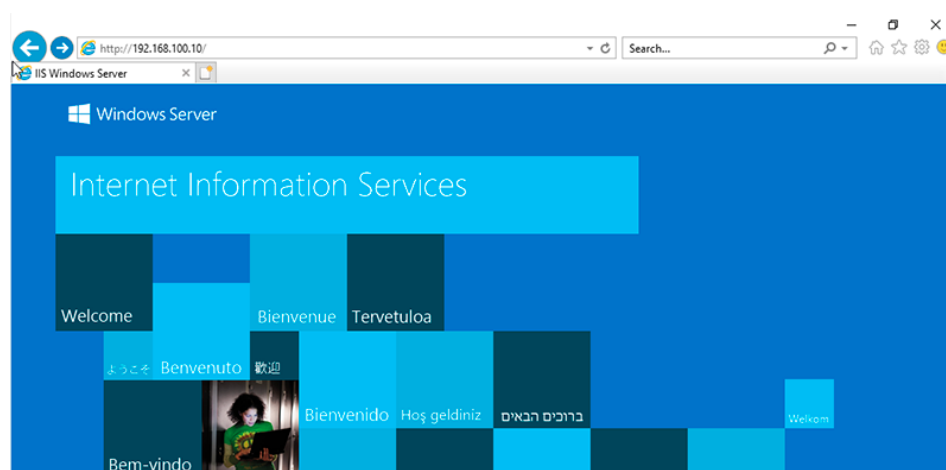


Figura 13 – Instalação do Web Server (IIS).

Após a instalação dos recursos do Web Server, já é possível acessá-lo de qualquer browser da rede local por seu número IP.



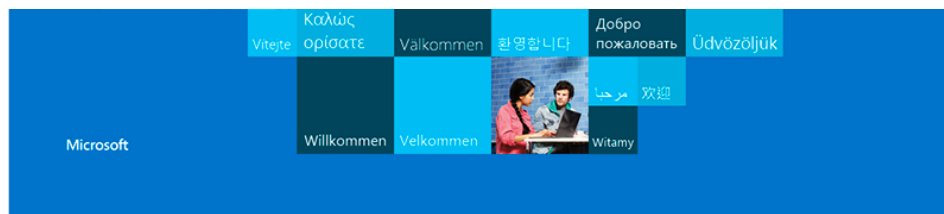


Figura 14 – Página web padrão do servidor web acessível via browser pelo IP 192.168.100.10.

Observe que um site de teste é apresentado, sendo possível alterá-lo para o site desejado após a instalação.

4.2.2 Sites

Um site é um local, uma pasta em um servidor web. Em um mesmo servidor, é possível ter vários sites diferentes. Talvez seu site preferido esteja hospedado no mesmo servidor de outro site de sua preferência. Vamos entender como este procedimento é realizado.

Com a instalação do IIS, uma pasta padrão no Windows Server é criada no caminho C:\inetpub\wwwroot.

Nesta pasta, no servidor é possível observar os arquivos do site de teste do IIS.

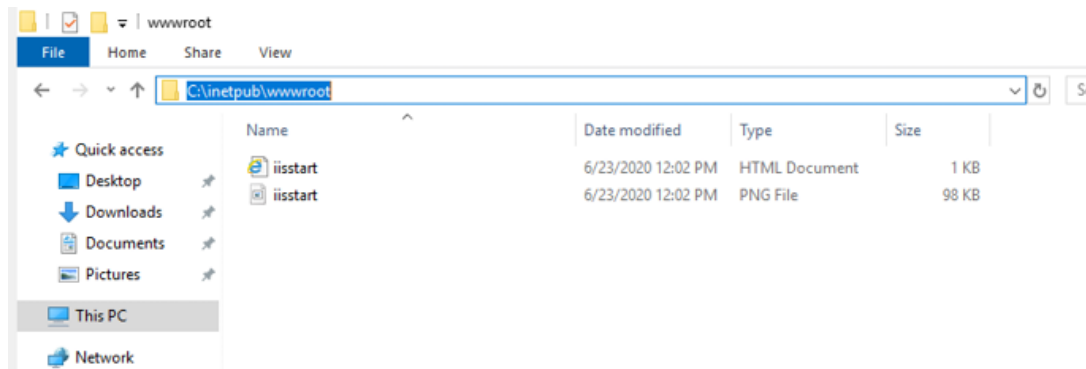


Figura 15 – Local de hospedagem padrão do web server.

O próximo passo é substituir estes arquivos pelos arquivos do site desejado.

Então o próximo passo é hospedar o conteúdo e esse conteúdo certamente não será criado por você, e sim por um webdesigner ou por uma produtora de conteúdo. Evite cair na tentação de criar você mesmo o site da empresa. Os sites atuais são repletos de recursos e tomam muito tempo entre o projeto e a implementação. É preciso conhecer html, asp ou php, banco de dados, linguagem SQL, tratamento de imagens para a Internet, JavaScript, APIs etc. É outra área, outra profissão e deve ficar a cargo de outro profissional. Suas atribuições após a instalação do IIS são cuidar para que o conteúdo seja publicado corretamente, manter o site seguro e sempre trabalhar em parceria com o desenvolvedor do site (THOMPSON, 2014, p. 253).

Realizando a substituição dos arquivos, este novo conteúdo pode ser acessado por qualquer máquina cliente da rede, através do número IP ou do nome do servidor, ou ainda por outra configuração de registro configurada previamente no serviço de DNS na rede local. O acesso deste servidor externamente demanda configurações e recursos para que este servidor esteja disponível externamente.

Como não criamos um site registrado no Registro.br, o conteúdo do IIS nos exemplos só estará disponível para a rede local, acessado pelo endereço IP ou pelo nome de domínio do AD. Intranet é o nome dado à hospedagem de site que só fica visível dentro da rede local. Com a instalação do IIS você possui as bases da Intranet, restando apenas desenvolver o conteúdo, geralmente um portal ou página Web com informações destinadas aos funcionários e usuários da rede local. Quando a Intranet é conectada à Internet e pode ser acessada de fora da rede local, ela se chama Extranet. Desta forma, a empresa pode manter um portal ou site de acesso restrito aos funcionários e fornecedores e outro site aberto ao público. É comum incluir a palavra **intra** ou **intranet** no endereço, por exemplo, **http://intranet.empresa.com** ou **http://www.empresa.com/intranet**. (THOMPSON, 2014, p. 254-255)

Após a instalação do IIS e a hospedagem dos arquivos do site, é possível realizar as personalizações adequadas pelo painel de administração do servidor web.

4.2.3 Administração

A administração de um servidor web pode ser feita pela ferramenta IIS Manager, que pode ser acessada pelo menu **Tool**, disponível no Server Manager do Windows Server 2019.

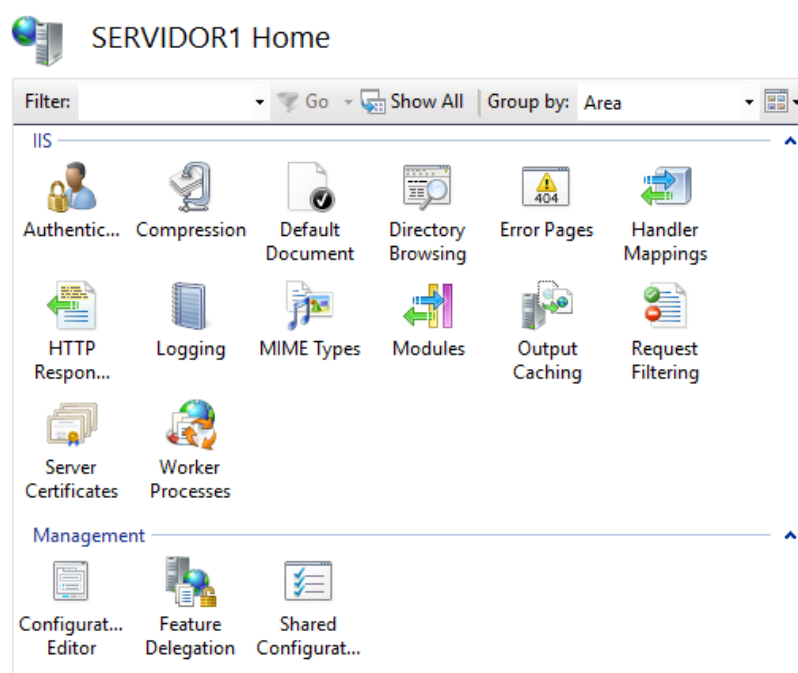


Figura 16 – Ferramentas administrativas do IIS.

Essa ferramenta apresenta os serviços de manutenção e diagnóstico que são bastante úteis para o administrador. Segundo Thompson (2014), as principais opções da ferramenta são:

Principais opções de ferramentas

» Clique nas abas para saber mais sobre o assunto

TTP	Ferramentas de Log	Monitor de solicitações	Rastreando	Log persona
-----	--------------------	-------------------------	------------	-------------

As ferramentas de administração também apresentam recursos de segurança e acesso a páginas da internet ou intranet. As opções presentes na ferramenta abrangem autenticação de usuários e recursos para configuração de proxy.



VOCÊ SABIA?

Possuir uma grande quantidade de servidores (data center) em uma rede local pode ser muito custoso para as empresas. Hoje, para alguns serviços de rede, é possível ter um servidor em nuvem, disponível de qualquer local, por um custo mais baixo do que ter um servidor físico. Isso é possível utilizando ferramentas como o Microsoft Azure, da Microsoft. Para mais informações e tutoriais de como realizar este procedimento, utilize o link a seguir: < <https://docs.microsoft.com/pt-br/learn/browse/?roles=administorator&products=azure> >

4.3 IPAM

O IPAM – IP Address Management (em português, Gerenciamento de endereços IP) é uma administração feita por software para controle de IPs entregues via DHCP. Em uma grande infraestrutura é ideal saber quais endereçamentos IPs foram entregues para qual dispositivo, além de saber quantos endereçamentos IPs ainda estão disponíveis para entrega. Os relatórios produzidos pelas ferramentas de IPAM podem prevenir abusos e acessos indevidos à rede, identificando possíveis hosts não autorizados a consumirem recursos da rede local.

4.3.1 Visão geral

O Windows Server apresenta sua própria ferramenta de IPAM. A ferramenta está disponível desde a versão 2012 do sistema operacional. Com ela, é possível gerenciar a entrega de endereçamento IPs via DHCP, além de controlar os IPs e nomes de computadores do serviço de DNS.

4.3.2 Gerenciando

O gerenciamento da ferramenta IPAM no Windows Server 2019 é feito após a sua instalação. Veja no tópico 4.4.1, quais são os pré-requisitos para a instalação da ferramenta, já sabendo que a infraestrutura deve ter um servidor DHCP em funcionamento. A ferramenta centraliza em um só local toda a gerência de escopos, junto à sua criação e exclusão. O diferencial da ferramenta é apresentar a utilização da entrega de cada escopo criado na infraestrutura e também apresentar relatórios não só para as ferramentas DHCP, mas também para o serviço DNS, podendo, pela ferramenta, criar e excluir zonas primárias de DNS e criar e editar novos registros.



VOCÊ SABIA?

Para mais informações sobre o gerenciamento DNS na ferramenta IPAM, consulte as informações da documentação oficial no link abaixo:

< <https://docs.microsoft.com/pt-br/windows-server/networking/technologies/ipam/add-a-dns-resource-record> >.

4.4 Instalação IPAM

A instalação do IPAM pode ser feita através do assistente *Add Roles and Features*, presente no Server Manager. Não é obrigatório o uso da ferramenta da Microsoft. Outras empresas também fornecem ferramentas com os mesmos recursos. Dentre elas, podemos destacar a SolarWinds (ferramenta comercial paga) e o PHPIPAM, sendo esta gratuita e caracterizada como um software do tipo *open-source*.

4.4.1 Requisitos

O IPAM conta com uma série de tecnologias de gerenciamento remoto para fornecer uma funcionalidade completa da ferramenta. A comunicação com vários elementos de rede em toda a empresa é necessária para a coleta de dados e o gerenciamento da configuração. Dependendo do escopo dos elementos gerenciados, essa comunicação pode precisar atravessar vários limites ou domínios de segurança. Sabendo disso, é importante também saber que, caso a infraestrutura possua recursos de segurança como firewalls e antivírus, eles devem estar devidamente configurados, com os protocolos utilizados pelo IPAM devidamente liberados para a ferramenta.

O ideal é que o IPAM seja instalado em um computador membro do domínio, sabendo que não é possível instalar o IPAM em um servidor controlador de domínio (ADDS).

Um servidor com o serviço IPAM instalado fornece suporte para uma única floresta do Active Directory. Topologias multi florestas não são suportadas pela ferramenta.

4.4.2 Cenário

Vamos visualizar um exemplo. Neste cenário, possuímos um domínio chamado de **empresa.local** com um servidor, chamado servidor1, como controlador de domínio que também agrega o servidor de DHCP e IIS. Temos também um segundo servidor, chamado de servidor2, adicionado a este domínio, no qual instalaremos a ferramenta IPAM da Microsoft.

No assistente de instalação de funções e recursos do Windows Server, na etapa Features (Recursos) o IPAM pode ser instalado selecionando o item **IP Address Managment (IPAM) Server**, tal como indicado na Figura 17.

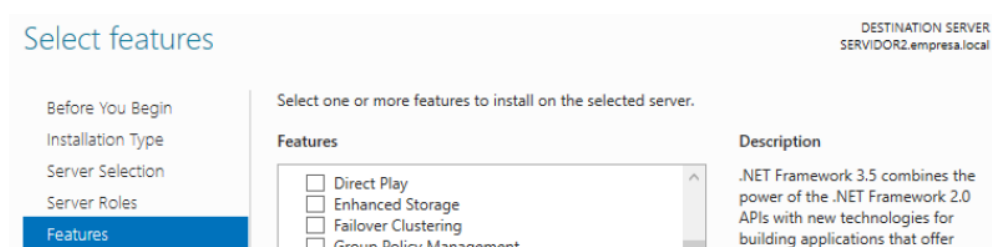




Figura 17 – Instalação do IPAM no Windows Server 2019.

Após a instalação dos recursos necessários, é necessário realizar a configuração inicial da ferramenta. Isso pode ser feito clicando no novo item IPAM, agora presente no Server Manager.

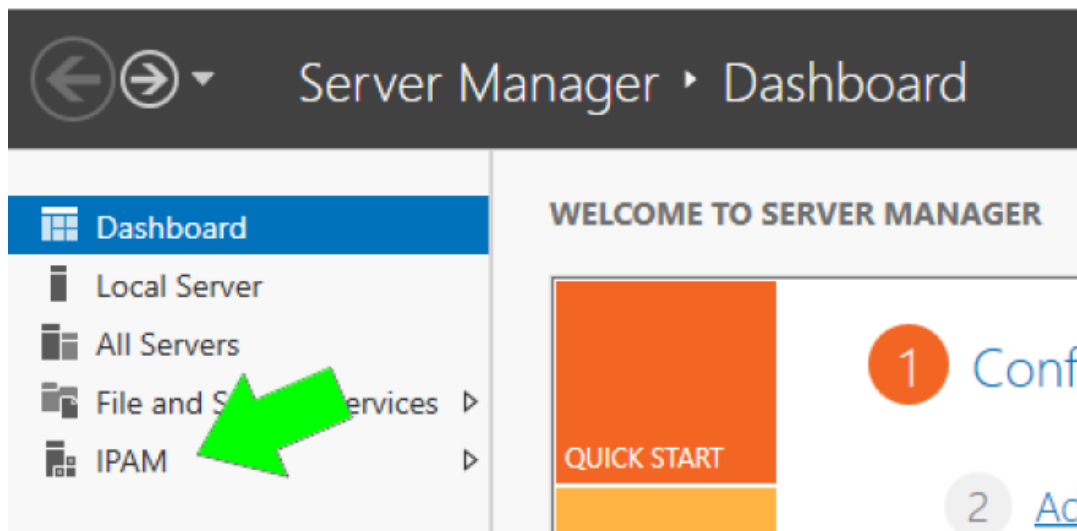


Figura 18 – Acesso a administração do IPAM no Windows Server 2019.

A configuração consiste em seis passos, sendo que o primeiro já definido: a conexão deste servidor como o servidor IPAM.

- 1 Connect to IPAM server
Connected to SERVIDOR2.EMPRESA.LOCAL
Connected as SERVIDOR2\Administrator
- 2 Provision the IPAM server
- 3 Configure server discovery
- 4 Start server discovery
- 5 Select or add servers to manage and verify IPAM
- 6 Retrieve data from managed servers

Figura 19 – Configuração necessária para o serviço IPAM.

» Clique nas setas ou arraste para visualizar as imagens

Na segunda etapa *Provision the IPAM server* (Provisionamento do servidor IPAM), é necessário indicar onde será salvo os logs do servidor IPAM. Pode-se definir um banco de dados locais para isso ou utilizar uma conexão com Microsoft SQL Server, caso esteja disponível.

Também é necessário indicar o nome da GPO que será utilizada para o gerenciamento do DHCP e DNS pela ferramenta.

A terceira etapa, *Configure Server Discovery* (configurar a detecção do servidor), é aquela na qual se deve definir a floresta e o domínio em que a ferramenta de IPAM atuará. Neste exemplo, o domínio **empresa.local** foi selecionado.

Select the forest:

empresa.local

Select domains to discover:

Select the server roles to discover:

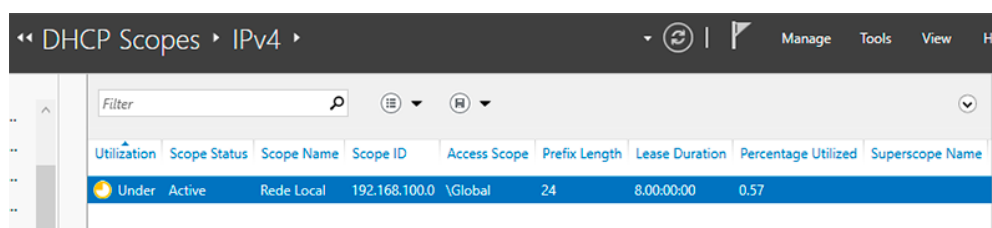
Domain	Domain controller	DHCP server	DNS server
(root domain) empresa.local	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Figura 20 – Definição do domínio a ser administrado.

A quarta etapa, *Start Server Discovery* (Iniciar a detecção do servidor), é utilizada para testar o funcionamento da implementação da ferramenta de IPAM. Ao clicar sobre a quarta etapa, deve-se aguardar que todas as ferramentas sejam instaladas nos servidores.

Na quinta etapa, *Select or add servers to manage and verify IPAM access* (Selecione ou adicione servidores para gerenciar e verificar o acesso ao IPAM), devem ser dadas as devidas permissões para que o servidor tenha acesso ao domínio e ao DHCP, para que os relatórios sejam gerados pela ferramenta.

A sexta e última etapa, *Retrieve data from managed servers* (Recuperar dados de servidores gerenciados), é utilizada para atualizar todos os dados dos servidores DNS e DHCP. Após isso, é possível visualizar os relatórios e administrar as entregas de IPs pela ferramenta:



The screenshot shows the 'DHCP Scopes > IPv4' window. It features a table with columns: Utilization, Scope Status, Scope Name, Scope ID, Access Scope, Prefix Length, Lease Duration, Percentage Utilized, and Superscope Name. One row is visible with the following data: Utilization (Under), Scope Status (Active), Scope Name (Rede Local), Scope ID (192.168.100.0), Access Scope (\Global), Prefix Length (24), Lease Duration (8.00:00:00), Percentage Utilized (0.57), and Superscope Name.

Utilization	Scope Status	Scope Name	Scope ID	Access Scope	Prefix Length	Lease Duration	Percentage Utilized	Superscope Name
Under	Active	Rede Local	192.168.100.0	\Global	24	8.00:00:00	0.57	

Figura 21 – Visualização de relatório de entrega de IPs.

No exemplo da figura 21, temos um escopo com o nome de “Rede Local”, que está ativo no servidor DHCP. O relatório demonstra a porcentagem de IPs entregues na coluna *Percentage Utilized* . Neste exemplo, contando com apenas 0.57% dos endereçamentos IPs entregues.

A ferramenta também apresenta inventários para a consulta de IPs expirados e duplicados. Além disso, é possível utilizá-la para criar novos escopos de entrega de endereçamento IP e novas zonas e ponteiros DNS.



VOCÊ SABIA?

Para mais informações sobre a instalação e o gerenciamento da ferramenta IPAM, sempre consulte a documentação oficial. No link abaixo, você encontrará referências de instalação e gerenciamento:<
<https://docs.microsoft.com/pt-br/windows-server/networking/technologies/ipam/manage-ipam> >.

Síntese

Nesta unidade, aprendemos as formas de configuração e de entregas automáticas de endereçamento IP, além de como devemos proceder para a administração dessas mesmas entregas. Conhecemos as classes de endereçamento IP e as versões disponíveis; aprendemos que essa configuração é de extrema importância para o funcionamento adequado da rede e é de responsabilidade do administrador manter a qualidade e o bom funcionamento do sistema. Conhecemos o modo de instalação e gerenciamento de um servidor web, utilizando a ferramenta da Microsoft chamada IIS, e, finalmente, descobrimos que um servidor web pode hospedar arquivos que estão disponíveis para os hosts da rede via intranet e que, eventualmente, também poderão ser acessados externamente via internet.

Referências bibliográficas

ADICIONAR um registro de recursos de DNS. **Microsoft** . 09 abr. 2020. Disponível em: <
<https://docs.microsoft.com/pt-br/windows-server/networking/technologies/ipam/add-a-dns-resource-record> >.
Acesso em: 27 jul. 2020.

TANENBAUM, A. S. **Sistemas operacionais modernos** . 4.ed. São Paulo: Pearson, 2016.

SERAGGI, M. R. **Windows Server 2016** . 4.ed. São Paulo: Editora Senac, 2019.

THOMPSON, M. A. **Microsoft Windows Server 2012** : instalação, configuração e administração de redes. 2.ed. São Paulo: Érica, 2014.