Imprimir

FOCO NO MERCADO DE TRABALHO

GERÊNCIA DE DESEMPENHO, CONFIGURAÇÃO E CONTABILIZAÇÃO

Renato Cividini Matthiesen

Ver anotações

IMPLANTAÇÃO DE UM SISTEMA DE SNIFFIG

Implantação de um *sniffer* na rede através de um programa chamado Wireshark, com objetivo de monitorar e capturar pacotes de rede que passam pelo switch, que realiza a comutação central da rede, distribuindo as conexões para outro switch e roteador dos departamentos.



Fonte: Shutterstock.

Deseja ouvir este material?

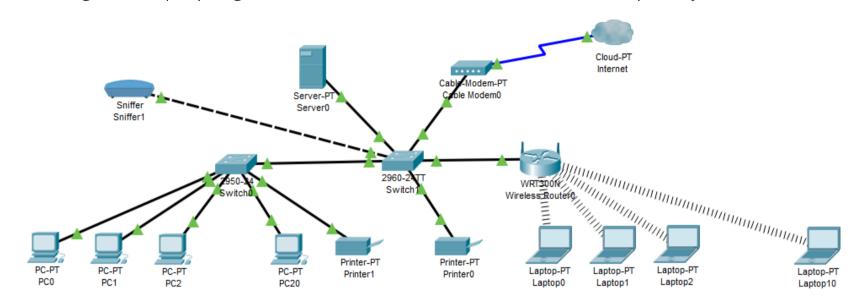
Áudio disponível no material digital.

SEM MEDO DE ERRAR

RELATÓRIO DO PROJETO DE REDES: MONITORAMENTO DE REDE VIA *SNIFFIG*

A solução para análise do tráfego de rede foi a implantação de um sniffer na rede através de um programa chamado Wireshark. O objetivo é monitorar e capturar pacotes de rede que passam pelo switch, que realiza a comutação central da rede, distribuindo as conexões para outro *switch* e roteador dos departamentos. A figura do *sniffer* apresentado na Figura 2.52 representa o dispositivo de hardware/software implantado na rede para análise e captura de pacotes. Este dispositivo é caracterizado por um computador munido do software farejador (sniffer).

Figura 2.52 | Topologia de rede do escritório de contabilidade com implantação de *sniffer*



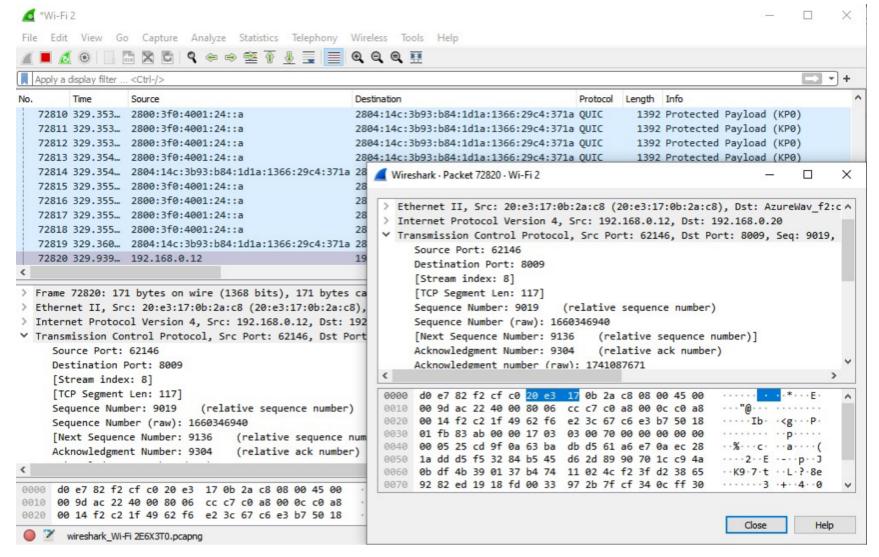
Fonte: elaborada pelo autor.

Em seguida, foram avaliadas informações coletadas através do software Wireshark, conforme Figura 2.53. O volume de informações é grande, considerando a intensidade das requisições na rede. A análise das requisições pode ser realizada através de filtros inseridos no programa, como HTTP (HyperText Transfer Protocol), que fará com que a ferramenta filtre apenas os pacotes do respectivo protocolo, ou ainda utilizar as ferramentas de estatística para análise.

Importante informar que a consultoria também pode utilizar outros programas de sniffig para fazer a avaliação dos dados capturados na rede, como o *Microsoft Network Monitor*, apresentado na Figura 2.53.

Figura 2.53 | Tela do *sniffer Wireshark* com informações de monitoramento de pacotes da rede

12/02/2022 09:19 lddkls211_red_sis_dis



Fonte: captura de tela da ferramenta *Wireshark* elaborada pelo autor.

Microsoft Network Monitor 3.4 File Edit View Frames Capture Filter Experts Tools Help 📄 New Capture 🤔 Open Capture 🔚 Save As 🛭 🐺 Capture Settings 🕨 Start 💵 Pause 🔳 Stop E Layout ▼ Parser Profiles ▼ Doptions W How Do I ▼ Capture 1 Start Page Parsers **Network Conversations** X Display Filter ■ MI Traffic Apply 🤻 Remove 🔀 History 🔻 🎖 Load Filter 🕶 Save Filter @ Clear Text My Traffic chrome.exe (16004) IPv6 (2804: 14C: 3B93: B84: 1D1A: 1 ± ♂ IPv4 (192.168.0.20 - 192.168.0.1 Pv4 (192. 168.0. 12 - 172.217. 173 Frame Summary - [Conversation Filter] ⊞ FV6 (2804:14C:38F9:6:0:0:0:11 🖳 Find 🔻 👃 🕇 📑 Autoscroll Color Rules 👫 Aliases 🕶 🔢 Columns √ IPv6 (2804: 14C: 3B93: B84: 1D1A: 1 Frame Number | Time Date Local Adjusted | Time Offset | Process Name | Source √ IPv6 (2804: 14C: 3B93: B84: 1D1A: 1 14:29:21 20/11/2020 724.4832355 chrome.exe 2804: 14C: 3B93: B84: 1D1A:.. 2804:14C:3BF... TCP TCP:Flags=...A...., SrcPort=61997, DstPort=HTTPS(443), P. 148319 14:29:21 20/11/2020 724.4832652 chrome.exe 724.4835052 chrome.exe 2804:14C:3BF9:6:0:0:0:11 2804:14C:3B9... TCP TCP:[Continuation to #147859]Flags=...A...., SrcPort=HTT.. TCP:[Continuation to #147859]Flags=...A...., SrcPort=HTT... Pv4 (192.168.0.12 - 151.101.93. 148320 14:29:21 20/11/2020 2804:14C:3BF9:6:0:0:0:11 2804:14C:3B9... TCP:[Continuation to #147859]Flags=...A..., SrcPort=HTT.
TCP:Flags=...A..., SrcPort=61997, DstPort=HTTPS(443), P.
TCP:[Continuation to #147859]Flags=...A..., SrcPort=HTT.
TCP:[Flags=...A..., SrcPort=61997, DstPort=HTTPS(443), P.
TCP:[Reep alive]Flags=...A..., SrcPort=62009, DstPort=H.
TCP:[Keep alive]Flags=...A..., SrcPort=61867, DstPort=H. 148321 14:29:21 20/11/2020 724. 4836394 chrome.exe 724. 4838025 chrome.exe 724. 4848960 chrome.exe 724. 485460 chrome.exe 724. 485540 chrome.exe 724. 48554727 chrome.exe 724. 4855643 chrome.exe 724. 4855643 chrome.exe 724. 4856643 chrome.exe 725.0506280 chrome.exe 726.50562839 chrome.exe 728.5264758 chrome.exe 724.4836394 chrome.exe 2804: 14C: 3B93: B84: 1D1A: 2804:14C:3BF... 148322 14:29:21 20/11/2020 2804:14C:3BF9:6:0:0:0:11 2804:14C:3B9... TPv4 (192. 168.0. 12 - 151. 101.94. 148323 14:29:21 20/11/2020 2804:14C:3BF9:6:0:0:0:11 2804:14C:3B9... 14:29:21 20/11/2020 14:29:21 20/11/2020 14:29:21 20/11/2020 14:29:21 20/11/2020 14:29:21 20/11/2020 14:29:21 20/11/2020 14:29:22 20/11/2020 14:29:22 20/11/2020 14:29:22 20/11/2020 14:29:25 20/11/2020 14:29:25 20/11/2020 148324 2804:14C:3BF9:6:0:0:0:11 2804:14C:3B9... Pv4 (192.168.0.12 - 151.101.94. 148325 2804:14C:3BF9:6:0:0:0:11 2804:14C:3B9... 2804:14C:389... 2804:14C:389... 2804:14C:389... 2804:14C:38F... 2804:14C:38F... 2804:14C:38F... 148326 2804:14C:3BF9:6:0:0:0:11 148327 2804: 14C: 3BF9:6:0:0:0:11 2804: 14C: 3B93: B84: 1D1A: . 2804: 14C: 3B93: B84: 1D1A: . Pv4 (192.168.0.12 - 201.7.182.2 TPv4 (192.168.0.12 - 186.192.91. TLS:TLS Rec Layer-1 SSL Application Data TPv4 (192.168.0.12 - 201.7.182.1 ± ... ♂ IPv4 (192.168.0.12 - 104.125.127 TPv4 (192.168.0.12 - 35.201.123. X Hex Details Frame Details ± ... of IPv6 (2804:14C:3B93:B84:1D1A:1 Frame: Number = 148390, Captured Frame Length = 116, MediaType = Pv4 (192.168.0.12 - 201.7.182.1 ैं≓ै Decode As ■ Width ▼ Prot Off: 0 (0x00) Frame Off: 0 (0x00) Sel Bytes: (WiFi: [Unencrypted Data] F.....P, (I) RSSI = -29 dBm, Rate = 3. ⊕ ♂ IPv4 (192.168.0.12 - 186.192.81. 000 02 20 00 04 00 00 00 00 00 00 00 LLC: Unnumbered(U) Frame, Command Frame, SSAP = SNAP(Sub-Networ Pv4 (192.168.0.12 - 131.0.25.19 Snap: EtherType = Internet IP (IPv4), OrgCode = XEROX CORPORATION 0016 ⊕ JPv4 (192. 168.0. 12 - 104. 125. 115 FF 07 01 AE 7B B1 62 BF D6 01 08 ÿ.. ®{±b¿Ö. √ IPv4 (192. 168.0. 12 - 186. 192.81. Ipv4: Src = 151.101.94.133, Dest = 192.168.0.12, Next Protocol = 0021 ⊕ of IPv6 (2804:14C:3B93:B84:1D1A:1 Tcp: [Keep alive ack]Flags=...A...., SrcPort=HTTPS(443), DstPort 002C 4F CB 6F 2A 8C 44 4F CB 6F 28 20 0Ëo* DOËo(JPv4 (192.168.0.12 - 18.205.75.1 ⊕ ♂ IPv4 (192.168.0.12 - 131.0.25.12 00 34 06 37 40 00 38 06 85 EE 97 .4.7@.8. î 0042

Figura 2.54 | Tela do *Microsoft Network Monitor*

Fonte: captura de tela do *Microsoft Network Monitor* elaborada pelo autor.

Displayed: 124335 Dropped: 0

Captured: 148778 Pending: 67

Avaliando os dados coletados via software *sniffer*, pode-se perceber os acessos dos hosts ativos no ambiente de rede, por exemplo, as requisições e os acessos do endereço IP 192.168.0.12.

O relatório pode ser completado com análises mais detalhadas.

Version 3.4.2350.0

Ver anotações

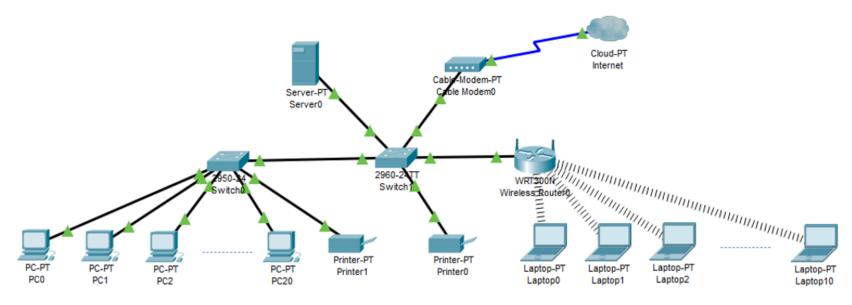
ANÁLISE DE DISPONIBILIDADE DE REDE DE COMPUTADORES DE UM ESCRITÓRIO DE CONTABILIDADE

O escritório de contabilidade avaliado via consultoria de tecnologia de informação mantém sua rede de computadores instalada, a qual suporta todas as atividades profissionais desenvolvidas no ambiente interno para cerca de 30 estações de trabalho (desktops e notebooks). Esta rede oferece a infraestrutura de hardware e software para utilização de sistemas instalados em seu servidor (Server0), softwares instalados localmente nas estações de trabalho, assim como sistemas acessados via browser de internet para operação dentro dos conceitos de SaaS (Software as a Service), dentro de tecnologias de nuvem, como os sistemas oferecidos pela Receita Federal, entre outros. Durante todo o ano, o escritório desenvolve atividades de consultoria e gestão contábil para mais de 500 empresas da cidade onde atua, sendo que a comunicação via e-mail e sistemas de mensagens eletrônicas instantâneas e a troca de documentos são intensas e ocorrem diariamente, de segunda a sexta-feira. Este escritório de contabilidade oferece também aos seus clientes um repositório de informações via Web Service, por meio do qual seus clientes podem se orientar para as atividades administrativas de suas empresas.

Considerando as informações apresentadas, esse escritório necessita de um sistema que tenha uma disponibilidade alta durante seis dias da semana, sendo possível sua indisponibilidade apenas aos domingos, dia da semana em que o sistema não necessariamente precisa estar disponível. Dentro deste cenário, a disponibilidade da rede deve operar durante os 365 dias do ano, com exceção dos domingos. A Figura 2.55 apresenta a topologia da rede para planejamento da sua disponibilidade.

A sua equipe de consultoria em tecnologia da informação foi contratada para gerar um relatório, no qual se apresentará a disponibilidade calculada deste sistema de redes de computadores necessária. Estruture seus cálculos em um relatório chamado de Consultoria em gerenciamento de redes: disponibilidade da rede.

Figura 2.55 | Topologia de rede do escritório de contabilidade



Fonte: elaborada pelo autor.

<u>RESOLUÇÃO</u>

0

Relatório de consultoria em gerenciamento de redes: disponibilidade da rede

Para fazer os cálculos de disponibilidade da rede do escritório de contabilidade, necessitamos aplicar a fórmula:

D = MTTF / (MTTF + MTTR)

Onde:

D é disponibilidade.

MTTF (*Mean Time to Failure*) é o tempo médio para falha, ou seja, tempo de operação da rede no período.

MTTR (*Mean Time to Repair*) é o tempo médio para reparo.

O escritório precisa operar 365 dias no ano, exceto aos domingos. Isto significa que o ano tem 365 dias - 52 domingos.

Vamos calcular em horas: (365 * 24) – (52 * 24) = 8760 – 1248 = 7512.

Temos, assim, MTTF = 7512 e MTTR = 1248.

D = MTTF / (MTTF + MTTR)

D = 7512 / (7512 + 1248)

D = 7512 / 8760

D = 0.85753.

Temos uma disponibilidade necessária de 85,7%.

lddkls211_red_sis_dis

Ver anotações

0