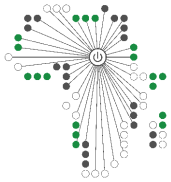


Universidade Virtual Africana

INFORMÁTICA APLICADA: CSI 5300

ADMINISTRAÇÃO DE REDES DE COMPUTADORES

Ambrósio Patrício Vumo

Prefácio

A Universidade Virtual Africana (AVU) orgulha-se de participar do aumento do acesso à educação nos países africanos através da produção de materiais de aprendizagem de qualidade. Também estamos orgulhosos de contribuir com o conhecimento global, pois nossos Recursos Educacionais Abertos são acessados principalmente de fora do continente africano.

Este módulo foi desenvolvido como parte de um diploma e programa de graduação em Ciências da Computação Aplicada, em colaboração com 18 instituições parceiras africanas de 16 países. Um total de 156 módulos foram desenvolvidos ou traduzidos para garantir disponibilidade em inglês, francês e português. Esses módulos também foram disponibilizados como recursos de educação aberta (OER) em oer.avu.org.

Em nome da Universidade Virtual Africana e nosso patrono, nossas instituições parceiras, o Banco Africano de Desenvolvimento, convido você a usar este módulo em sua instituição, para sua própria educação, compartilhá-lo o mais amplamente possível e participar ativamente da AVU Comunidades de prática de seu interesse. Estamos empenhados em estar na linha de frente do desenvolvimento e compartilhamento de recursos educacionais abertos.

A Universidade Virtual Africana (UVA) é uma Organização Pan-Africana Intergovernamental criada por carta com o mandato de aumentar significativamente o acesso a educação e treinamento superior de qualidade através do uso inovador de tecnologias de comunicação de informação. Uma Carta, que estabelece a UVA como Organização Intergovernamental, foi assinada até agora por dezenove (19) Governos Africanos - Quênia, Senegal, Mauritânia, Mali, Costa do Marfim, Tanzânia, Moçambique, República Democrática do Congo, Benin, Gana, República da Guiné, Burkina Faso, Níger, Sudão do Sul, Sudão, Gâmbia, Guiné-Bissau, Etiópia e Cabo Verde.

As seguintes instituições participaram do Programa de Informática Aplicada: (1) Université d'Abomey Calavi em Benin; (2) Université de Ougagadougou em Burkina Faso; (3) Université Lumière de Bujumbura no Burundi; (4) Universidade de Douala nos Camarões; (5) Universidade de Nouakchott na Mauritânia; (6) Université Gaston Berger no Senegal; (7) Universidade das Ciências, Técnicas e Tecnologias de Bamako no Mali (8) Instituto de Administração e Administração Pública do Gana; (9) Universidade de Ciência e Tecnologia Kwame Nkrumah em Gana; (10) Universidade Kenyatta no Quênia; (11) Universidade Egerton no Quênia; (12) Universidade de Addis Abeba na Etiópia (13) Universidade do Ruanda; (14) Universidade de Dar es Salaam na Tanzânia; (15) Universite Abdou Moumouni de Niamey no Níger; (16) Université Cheikh Anta Diop no Senegal; (17) Universidade Pedagógica em Moçambique; E (18) A Universidade da Gâmbia na Gâmbia.

Bakary Diallo

O Reitor

Universidade Virtual Africana

Créditos de Produção

Autor

Ambrósio Patrício Vumo

Par revisor(a)

Adilis Pereira

UVA - Coordenação Académica

Dr. Marilena Cabral

Coordenador Geral Programa de Informática Aplicada

Prof Tim Mwololo Waema

Coordenador do módulo

Robert Oboko

Designers Instrucionais

Elizabeth Mbasu

Benta Ochola

Diana Tuel

Equipa Multimédia

Sidney McGregor

Barry Savala

Edwin Kiprono

Kelvin Muriithi

Victor Oluoch Otieno

Michal Abigael Koyier

Mercy Tabi Ojwang

Josiah Mutsogu

Kefa Murimi

Gerisson Mulongo

Direitos de Autor

Apoiado por

Projeto Multinacional II da UVA financiado pelo Banco Africano de Desenvolvimento.

Tabela de conteúdo

Descrição Geral do Curso

Bem-vindo(a) a Administração de Redes de Computadores

Bem-vindo ao módulo de Administração de Redes de computadores: Cada vez mais, pessoas e organizações dependem da disponibilidade de redes de computadores para o desempenho das mais diversas actividades, sejam elas profissionais, académicas ou de lazer. As redes de computadores tornaram-se numa peça fundamental de qualquer sistema de informação. A crescente dimensão, heterogeneidade e complexidade dos ambientes distribuídos exige que a concepção, realização e operação de uma rede de computador tenha em consideração um conjunto de mecanismos e ferramentas para a monitorização e controlo dos recursos de comunicação. A gestão de redes consiste no conjunto de funções para controlar, planear, alocar, implementar, coordenar e monitorizar os recursos de rede. A gestão de uma rede de computadores torna-se uma actividade essencial para garantir o seu funcionamento contínuo assim como para assegurar um elevado grau de qualidade dos serviços oferecidos. Diversos modelos foram criados para possibilitar a gestão de redes, dados e telecomunicações dos quais se destacam o FCAPS (Fault, Configuration, Accounting, Performance and Security) por servir de base para os demais modelos.

Falta a descrição do curso. O que contém este curso?

Pré-requisitos

Para fazer este curso deverá ter estudado anteriormente:

Redes de computadores e comunicação de dados

Introdução a segurança Informática

Materiais

Os materiais necessários para completar este curso incluem:

[1] José Maurício Pinheiro, Infra-Estrutura Eléctrica para Rede de Computadores, 1st ed., Ciência Moderna, Ed., 2008.

[2] Raj Jain, The Art of Computer Systems Performance Analysis: Techniques for experimental design, measurement, simulation and modeling, Wiley And Sons, Ed. York New, 1991.

[3] James D. Mccabe, Network Analysis, Architecture, and Design, 3rd ed. Burlington: Morgan Kaufmann, 2007.

[4] William Stallings, SNMP, SNMPv2, SNMPv3 and RMON1 and 2, 3rd ed., Addison Wesley Longman, Ed., 1999.

[5] Douglas R. Mauro, Kevin J. Schmidt, Help for system and network administrators:

Essential SNMP, 1st ed. America: O'Reilly & Associates, 2001.

[6] Véstias Mário, Redes CISCO para profissionais, 4th ed., FCA, Ed. Lisboa, Portugal, 2009.

[7] Willig Andreas, "Performance Evaluation Techniques," Summer 2004, April 2005.

[8] Richard Blum, Network Performance Open Source Toolkit: Using Netperf, tcptrace, NIST Net, and SSFNet, Carol Long, Ed. Indianapolis, United States: Wiley Publishing, 2003.

[9] Raj Jain, Hassan Mahbub, High performance tcp/ip networking concepts, issues and solutions, Prentice Hall, Ed., 2003.

[10] George Coulouris, Jean Dollimore, Tim Kindberg, Distributed Systems: Concepts and Design, 4th ed., Pearson Education Limeted, Ed. London, 2005.

[11] Carey Williamson, "Internet Traffic Measurement," IEEE Internet Computing, vol. 5, no. 6, p. 9, November 2001.

[12] Solange Lima, Network traffic measurement, 2009/2010, Textos de apoio ao Mestrado.

[13] Cacti. (2010, January) Cacti. [Online]. http://docs.cacti.net/

[14] Nagios. (2010, January) The Industry Standard in IT Infrastructure Monitoring. [Online]. http://www.nagios.com/products/nagiosxi/

[15] Ntop. (2010, March) Ntop. [Online]. http://www.ntop.org/documentation.html

[16] Mikrotik. (2010, January) DUDE. [Online]. http://www.mikrotik.com/thedude.php.

[17] Coppini Andrea. (2010, january) Buiding Custom Probes and Configuring devices via SNMP. [Online]. http://mum.mikrotik.com/presentations/CZ09/Building custom-probes-and-SNMP.pdf

[18] Edmundo Monteiro, Fernando Boavida, Engenharia de redes de informáticas, 8th ed., FCA, Ed. Lisboa, Portugal, 2000.

[19] José Gouveia, Alberto Magalhães, Redes de Computadores, 8th ed., FCA, Ed. Lisboa, Portugal, 2009.

Objetivos do Curso

Após concluir este curso, o(a) aluno(a) deve ser capaz de:

- Dar suporte Técnico de Hardware
- Gerir Redes de Comunicação;
- Consultor Técnico de administração de Redes
- Arquitecto de Redes de computadores
- Gestor de projectos de Redes de computadores

Unidades

Unidade 0: Diagnóstico

Esta unidade zero foi concebida para consciencializar os estudantes sobre a importância da área cada vez mais em destaque no contexto actual de redes de computadores e tecnologia de informação, assim, visa fornecer conhecimento especializado na definição, desenvolvimento e Administração de redes quer sobre plataformas de comunicação fixas quer móveis.

Unidade 1: Introdução

A crescente dimensão, heterogeneidade e complexidade dos ambientes distribuídos exige que a concepção, realização e operação de uma rede informática tenha em consideração um conjunto de mecanismos e ferramentas para a monitorização e controlo dos recursos de comunicação. A gestão de redes consiste no conjunto de funções para controlar, planear, alocar, implementar, coordenar e monitorizar os recursos de rede [3]. A gestão de uma rede de computadores torna-se uma actividade essencial para garantir o seu funcionamento contínuo assim como para assegurar um elevado grau de qualidade dos serviços oferecidos.

Unidade 2: Serviços de Redes

Serviços de redes fornecem serviços essenciais de suporte a redes de computadores. Estes diferem dos serviços normais utilizados pelo utilizadores finais, isto é, as aplicações em que eles são acessados diretamente pelos utilizadores finais. Em vez disso, esses serviços são usados por computadores em rede para simplificar algumas actividades por exemplo, instalação, configuração e operacionalização da propria rede. nesta unidade abordaremos topicos relacionadas com: serviço de configuração dinámica dos endereços IP (DHCP) , serviços de tradução de nomes (DNS), serviço de correios electronicos, servidor de ficheiros e servidores de impressão

Unidade 3: Ferramentas de Gestão de rede

Os serviços fornecidos pelo redes devem apresentar um nıvel acertável ou quase optimo de qualidade pois caso contrário corre-se o risco da rede não ser utilizada e gerar grande frustração junto de utilizadores e administradores. O esforço de instalação bem como os gastos efectuados serão perdidos e a rede tornarse-â inviável. E essencial dotar em

ferramentas e mecanismos que permitam monitorar e corrigir situações anômalas que possam surgir durante a operação, de forma a aumentar o grau de confiança que o serviço apresenta face aos seus utilizadores, nesta unidade é dedicado à apresentação dos principais conceitos relativos a medição e monitorização de redes de computadores.

Unidade 4: Segurança de hardware e Software

A segurança da rede é o processo através do qual uma rede é protegida contra ameaças internas e externas de várias formas. A fim de desenvolver uma compreensão completa do que é segurança na rede, você deve entender as ameaças contra as quais a segurança da rede visa proteger uma rede. É igualmente importante para desenvolver um entendimento de alto nível dos principais mecanismos que podem ser postas em prática para impedir esses ataques

Unidade 5: Manutenção e resolução de problemas

Vamos concluir este modulo de administração de redes com um tópico que todos nós achamos que nunca precisaremos se preocupar, mas todos precisam saber. É quase impossível uma rede funcionar sem acontecer algo de errado. Isto é, não existem duas redes iguais mesmo se tiverem a mesma topologia. A resolução de problemas de uma rede local pode ser um trabalho sério e difícil de realizar. Muitas factores entram em jogo. Um problema que parece fácil de resolver pode pode tornar algo totalmente difícil de resolver. Algumas vezes uma a resolução do problema pode levar uma hora mas o mesmo problema a sua resolução pode levar um dia inteiro.

Assim nesta unidade irá aprender a .....

Avaliação

Em cada unidade encontram-se incluídos instrumentos de avaliação formativa a fim de verificar o progresso do(a)s estudantes.

No final de cada módulo são apresentados instrumentos de avaliação sumativa, tais como testes e trabalhos finais, que compreendem os conhecimentos construídos e as competências desenvolvidas ao estudar o módulo.

A implementação dos instrumentos de avaliação sumativa fica ao critério da instituição que oferece o curso. A estratégia de avaliação sugerida é a seguinte:

Unidade	Temas e Atividades	Estimativa do tempo
1	Consulta de materiais e outros recursos	04 Valores
2	Exercícios práticos	10 Valores
3	Avaliação formativa e relatório das actividades	06 Valores

Calendarização

Unidade	Temas e Atividades	Estimativa do tempo
Diagnostico	Teste de Diagnostico	4 Horas
Introdução	Exercícios	8 horas
Serviço de Redes	Exercícios	10 horas
Ferramentas de gestão de redes	Exercícios	18 horas
Segurança de Hardware e software	Exercícios	20 horas
Laboratório	Exercícios	10 Horas

Leituras e outros Recursos

As leituras e outros recursos deste curso são:

Unidade 0

Leituras e outros recursos obrigatórios:

[1] José Maurício Pinheiro, Infra-Estrutura Eléctrica para Rede de Computadores, 1st ed., Ciência Moderna, Ed., 2008.

[2] Raj Jain, The Art of Computer Systems Performance Analysis: Techniques for experimental design, measurement, simulation and modeling, Wiley And Sons, Ed. York New, 1991.

[3] James D. Mccabe, Network Analysis, Architecture, and Design, 3rd ed. Burlington: Morgan Kaufmann, 2007.

[4] William Stallings, SNMP, SNMPv2, SNMPv3 and RMON1 and 2, 3rd ed., Addison Wesley Longman, Ed., 1999.

[5] Douglas R. Mauro, Kevin J. Schmidt, Help for system and network administrators: Essential SNMP, 1st ed. America: O'Reilly & Associates, 2001.

Leituras e outros recursos opcionais:

[digite o título, o nome do(s) autor(es) e outras informações de referência]

[digite o título, o nome do(s) autor(es) e outras informações de referência]

Unidade 1

Leituras e outros recursos obrigatórios:

[1] José Maurício Pinheiro, Infra-Estrutura Eléctrica para Rede de Computadores, 1st ed., Ciência Moderna, Ed., 2008.

[2] Raj Jain, The Art of Computer Systems Performance Analysis: Techniques for experimental design, measurement, simulation and modeling, Wiley And Sons, Ed. York New, 1991.

[3] James D. Mccabe, Network Analysis, Architecture, and Design, 3rd ed. Burlington: Morgan Kaufmann, 2007.

[4] William Stallings, SNMP, SNMPv2, SNMPv3 and RMON1 and 2, 3rd ed., Addison Wesley Longman, Ed., 1999.

[5] Douglas R. Mauro, Kevin J. Schmidt, Help for system and network administrators: Essential SNMP, 1st ed. America: O'Reilly & Associates, 2001.

Leituras e outros recursos opcionais:

[digite o título, o nome do(s) autor(es) e outras informações de referência]

[digite o título, o nome do(s) autor(es) e outras informações de referência]

Unidade 2

Leituras e outros recursos obrigatórios:

[1] José Maurício Pinheiro, Infra-Estrutura Eléctrica para Rede de Computadores, 1st ed., Ciência Moderna, Ed., 2008.

[2] Raj Jain, The Art of Computer Systems Performance Analysis: Techniques for experimental design, measurement, simulation and modeling, Wiley And Sons, Ed York New, 1991.

[3] James D. Mccabe, Network Analysis, Architecture, and Design, 3rd ed. Burlington: Morgan Kaufmann, 2007.

[4] William Stallings, SNMP, SNMPv2, SNMPv3 and RMON1 and 2, 3rd ed., Addison Wesley Longman, Ed., 1999.

[5] Douglas R. Mauro, Kevin J. Schmidt, Help for system and network administrators: Essential SNMP, 1st ed. America: O'Reilly & Associates, 2001.

Leituras e outros recursos opcionais:

[digite o título, o nome do(s) autor(es) e outras informações de referência]

[digite o título, o nome do(s) autor(es) e outras informações de referência]

Unidade 3

Leituras e outros recursos obrigatórios:

[1] José Maurício Pinheiro, Infra-Estrutura Eléctrica para Rede de Computadores, 1st ed., Ciência Moderna, Ed., 2008.

[2] Raj Jain, The Art of Computer Systems Performance Analysis: Techniques for experimental design, measurement, simulation and modeling, Wiley And Sons, Ed.York New, 1991.

[3] James D. Mccabe, Network Analysis, Architecture, and Design, 3rd ed. Burlington:

Morgan Kaufmann, 2007.

[4] William Stallings, SNMP, SNMPv2, SNMPv3 and RMON1 and 2, 3rd ed., Addison

Wesley Longman, Ed., 1999.

[5] Douglas R. Mauro, Kevin J. Schmidt, Help for system and network administrators:

Essential SNMP, 1st ed. America: O'Reilly & Associates, 2001.

Leituras e outros recursos opcionais:

[digite o título, o nome do(s) autor(es) e outras informações de referência]

[digite o título, o nome do(s) autor(es) e outras informações de referência]

Unit 4

Leituras e outros recursos obrigatórios:

[1] José Maurício Pinheiro, Infra-Estrutura Eléctrica para Rede de Computadores, 1st

ed., Ciência Moderna, Ed., 2008.

[2] Raj Jain, The Art of Computer Systems Performance Analysis: Techniques for

experimental design, measurement, simulation and modeling, Wiley And Sons, Ed.

York New, 1991.

[3] James D. Mccabe, Network Analysis, Architecture, and Design, 3rd ed. Burlington:

Morgan Kaufmann, 2007.

[4] William Stallings, SNMP, SNMPv2, SNMPv3 and RMON1 and 2, 3rd ed., Addison

Wesley Longman, Ed., 1999.

[5] Douglas R. Mauro, Kevin J. Schmidt, Help for system and network administrators:

Essential SNMP, 1st ed. America: O'Reilly & Associates, 2001.

Leituras e outros recursos opcionais:

[digite o título, o nome do(s) autor(es) e outras informações de referência]

[digite o título, o nome do(s) autor(es) e outras informações de referência]

Unit 5

Leituras e outros recursos obrigatórios:

[1] José Maurício Pinheiro, Infra-Estrutura Eléctrica para Rede de Computadores, 1st ed., Ciência Moderna, Ed., 2008.

[2] Raj Jain, The Art of Computer Systems Performance Analysis: Techniques for experimental design, measurement, simulation and modeling, Wiley And Sons, Ed. York New, 1991.

[3] James D. Mccabe, Network Analysis, Architecture, and Design, 3rd ed. Burlington: Morgan Kaufmann, 2007.

[4] William Stallings, SNMP, SNMPv2, SNMPv3 and RMON1 and 2, 3rd ed., Addison Wesley Longman, Ed., 1999.

[5] Douglas R. Mauro, Kevin J. Schmidt, Help for system and network administrators: Essential SNMP, 1st ed. America: O'Reilly & Associates, 2001.

Leituras e outros recursos opcionais:

[digite o título, o nome do(s) autor(es) e outras informações de referência]

[digite o título, o nome do(s) autor(es) e outras informações de referência]

Unit 6

Leituras e outros recursos obrigatórios:

[1] José Maurício Pinheiro, Infra-Estrutura Eléctrica para Rede de Computadores, 1st ed., Ciência Moderna, Ed., 2008.

[2] Raj Jain, The Art of Computer Systems Performance Analysis: Techniques for experimental design, measurement, simulation and modeling, Wiley And Sons, Ed. York New, 1991.

[3] James D. Mccabe, Network Analysis, Architecture, and Design, 3rd ed. Burlington: Morgan Kaufmann, 2007.

[4] William Stallings, SNMP, SNMPv2, SNMPv3 and RMON1 and 2, 3rd ed., Addison

Wesley Longman, Ed., 1999.

[5] Douglas R. Mauro, Kevin J. Schmidt, Help for system and network administrators:

Essential SNMP, 1st ed. America: O'Reilly & Associates, 2001.

Leituras e outros recursos opcionais:

Unidade 0. Diagnóstico

Introdução à Unidade

Esta unidade zero foi concebida para consciencializar os estudantes sobre, área cada vez mais em destaque no contexto actual de redes de computadores e tecnologia de informação, assim, visa fornecer conhecimento especializado na definição, desenvolvimento e Administração de redes quer sobre plataformas de comunicação fixas quer móveis.

Objectivos da Unidade

Após a conclusão desta unidade, deverá ser capaz de:

- Avliar o seu conhecimento sobre o surgimento da actividades de gestão de redes de computadores
- Descrever a importância e vantagens de gestão de computadores
- Identificar principais serviços da rede a serem geridos

Termos-chave

Comunicação de dados: Transferência de informação entre unidades funcionais, através de transmissão de dados, segundo um protocolo.

Rede local: Rede de computadores situada no domínio privado de um utilizador e limitada geograficamente.

Partilha: utilização simultânea de um recurso por diferentes processos.

Protocolo: Conjunto de regras semânticas e sintácticas que regulam o comportamento das unidades funcionais durante a comunicação.

Topologia de rede: Arranjo esquemático das ligações e nós de uma rede.

Avaliação da Unidade

Verifique a sua compreensão!

Teste de Diagnóstico

Instruções

Este teste de diagnóstico permitirá verificar o estado dos conhecimentos dos alunos em relação ao módulo. Isso pode ajudar a orientar as actividades e a reorganizá-las

Critérios de Avaliação

A avaliação deverá processar-se de uma forma contínua, sistemática e periódica. O tipo de avaliação corresponderá aos objectivos definidos.

Avaliação

Segundo os requisitos abaixo apresentados, determine o plano de endereçamento segundo endereço de rede 200.100.50.0/24

a) 1 Sub-rede e 100 IP's

b) 1 Sub-rede e 40 IP's

c) 1 Sub-rede e 25 IP's

d) 4 Sub-rede e 4 IP's

Unidade 1. Introdução à Administração de Redes de Computadores

Introdução à Unidade

A crescente dimensão, heterogeneidade e complexidade dos ambientes distribuídos exige que a concepção, realização e operação de uma rede informática tenha em consideração um conjunto de mecanismos e ferramentas para a monitorização e controlo dos recursos de comunicação. A gestão de redes consiste no conjunto de funções para controlar, planear, alocar, implementar, coordenar e monitorizar os recursos de rede [3]. A gestão de uma rede de computadores torna-se uma actividade essencial para garantir o seu funcionamento contínuo assim como para assegurar um elevado grau de qualidade dos serviços oferecidos.

Objetivos da Unidade

Após a conclusão desta unidade, deverá ser capaz de:

- Fornecer uma visão geral da função e requisitos de administrador.
- Identificar as actividades de gestão de rede.
- Identificar a variedade de atividades administrativas.
- Distinguir e implementar as cinco àreas funcionais do modelo de gestão OSI.

Termos-chave

Gestão de Falhas: é detectar, registar e alertar os administradores do sistema de problemas que possam afectar as operações do mesmo.

Gestão de Configuração: é responsável pela monitorização das informações de configuração do sistema, e quaisquer mudanças que ocorram.

Actividades de Aprendizagem

Actividade 1.1 - Motivação

1.1.1 Introdução

A administração de redes surgiu com o crescimento das empresas e de seus parques de máquinas, as grandes empresas logo perceberam a necessidade de um profissional qualificado para exercer a função de manutenção de rede, bem como técnicos para o reparo de estações de trabalho e suporte aos usuários. Na década de 1970, com a popularização das estruturas de Centros Processamentos Dados, diversas profissões surgiram (e, hoje, algumas já não

existem mais!), como Scheduler de mainframe, programador, analista, etc. O administrador de redes também surgiu mais ou menos nessa época. A principal actividade de um administrador de redes é a mesma que um administrador de empresas, manter o sistema funcionando De preferência, sem parar, sem lentidão, sem utilizadores confusos e longe dos hackers.

1.1.2 Administração Pró-activa e Reactiva

Todo administrador de redes pode se comportar basicamente de duas formas:

Pró-activo: O administrador de redes deverá manter um cronograma de repação periódica de sua rede para saber como "andam as coisas" e não ter surpresas. Apenas ver o que está acontecendo não é o suficiente, existem, hoje, no mercado, diversas ferramentas que podem monitorar deste host, tráfego, estações de usuário, etc. e fornecer ao administrador relatórios sofisticados sobre o uso da rede. Vale a pena lembrar que estas ferramentas são caras, leva tempo para configurá-las e mais tempo ainda para interpretar a grande quantidade de informação que elas podem colectar dos objectos monitorados. As grandes empresas, geralmente por possuírem um orçamento maior, podem se dar o luxo de ter um profissional voltado exclusivamente para a monitoração da rede.

Re-activo: O administrador de redes está sempre apagando incêndios. A Empresa geralmente é pequena e este personagem está sempre carregado de tarefas que não deveria ser de sua competência como: dar suporte ao usuário, tirar dúvidas por telefone ou no local, dar manutenção em máquina do usuário, ajudar o chefe na sua apresentação no PowerPoint, pois a secretária faltou, etc. Resumindo: não importa o motivo, o administrador de redes nunca tem tempo para ler logs, instalar software de monitoração nem orçamento para isto. Então, quando um problema acontece, ele tenta resolver na hora.

Com relação à segurança, estes dois estilos de administração acarretam o seguinte:

O hacker tem mais trabalho para entrar em redes com administração pró-activa, acontece o oposto nas redes com administração reactiva;

As redes cujos administradores são reactivos só ficam sabendo que foram atacados muito tarde e, depois, não tem condições de se defenderem;

As redes com administração pró-activa, geralmente guardam logs de todas as actividades, podendo, assim, tentar pegar o hacker.

1.1.2 Principais Tarefas de um Administrador de Redes

Diariamente, o administrador de rede deverá realizar pelos menos algumas das seguintes tarefas:

Gerir contas de utilizadores: Criar contas, apagá-las, desabilitar temporariamente contas de utilizadores, configurá-las para que os usuários possam realizar o login sob determinadas condições, etc.

Adicionar/remover hardware de servidores: Manter o servidor actualizado, como por exemplo: instalar novos discos rígidos, update de Sistemas Operativos.

Adicionar/remover hardware de rede (router, hub, switch… etc): Manter a rede actualizada, troca de hubs, switchs, etc..

Realizar Backups: Realizar o backup de dados considerados importantes tanto para os usuários como para o funcionamento do sistema.

Instalar/actualizar novo software no servidor: Montar software do sistema atualizado e softwares usados pelos usuários.

Monitorar o sistema (Rede e/ou servidor): Realizar actividade de monitoramento dos servidores, redes, estações, etc., conforme definido em política de segurança.

Realizar Auditoria: Tarefa esta que deverá ser realizada de acordo com o que está escrito na política de segurança da empresa.

Resolver problemas no servidor/rede: Daemons que não estão bem configurados, etc

Manter documentação da rede (hosts, topologia, etc.): O administrador da rede não será sempre funcionário eterno e presente, um dia ele pode sair da empresa ou ficar doente, alguém deve entender como a rede funciona.

Ajudar os utilizadores no caso das pequenas empresas pois nas grandes existe um grupo de suporte aos utilizadores.

Onde está a Actividade 1.1?

Actividades de Aprendizagem

Actividade 1.2 - Aspectos Éticos

1.2.1 Introdução

O texto apresentado nas actividades anteriores nos permitiu compreender que a administração da rede requer habilidades técnicas impecáveis. Vamos ver quais são as exigências da profissão de administração de rede além de conhecimento técnico.

1.2.2 Aspectos Éticos

O exercício da profissão de administrador de rede, inegavelmente, tem uma dimensão ética que deve ser notificada e o respeito que deve ser tomada. Ética refere-se a todos os princípios de conduta que devem reger a vida em um grupo de pessoas. A moral que os resultados podem distinguir o que é bom e justo o que está errado e anti-natural.

Eticamente, é o respeito pela privacidade dos utilizadores e os interesses corporativos que são a principal preocupação no contexto das atividades administrativas. Em alguns duas situações podem ser rapidamente em conflito. Por exemplo, a administração da rede prossegue com a

análise de tráfego em relação ao gerenciamento de desempenho ou segurança da rede.

Esta análise pode revelar algumas informações sobre comunicações privadas e potencialmente incriminatórios de algumas pessoas no negócio. Outro exemplo é nas redes de comunicações móveis onde alguns administradores podem facilmente gerar histórico de comunicação de um determinado número de assinantes. Em suma, o administrador de rede tem o privilégio de ter acesso a informações sensíveis sobre os usuários e a empresa. Exigências éticas impostas para evitar qualquer uso de tais informações fora do âmbito estrito do exercício da sua função e não pode cair sem razões justificáveis nas mãos de terceiros, mesmo que se trate de seus superiores na empresa.

As questões éticas são geralmente geridas por códigos de ética desenvolvidos por algumas organizações profissionais e algumas empresas. No caso de administração de redes existe por exemplo, o código SAGE que define a ética do administrador de rede:

Onde está a Actividade 1.2 Aspectos éticos?

Actividades de Aprendizagem

Actividade 1.3 - Aspectos legais (de quê?)

1.3.1 Introdução

O administrador de rede é responsável pelo que acontece na rede da qual é responsável. Esta responsabilidade não se limita à ética: é também a legalidade (civil e penal).

1.3.2 Legislação

A modernização da legislação de se adaptar à era digital continua a ser um desafio para muitos Estados. No entanto, alguns países já têm legislação que define as actividades do administrador de rede, os seus direitos e deveres, bem como o quadro de implementação de certas atividades administrativas. A tendência emergente de casos conhecidos é que a lei geralmente permite medidas técnicas normalmente realizadas como parte de administração de rede: filtragem de tráfego por firewalls e outros sistemas, arquivo electrónico, através de sensores em locais de rede, e o uso de arquivos de log (registros), etc. No entanto, o administrador da rede está sujeito à obrigação de meios para proteger a privacidade e confidencialidade no que diz respeito aos dados pessoais a que tem acesso. Ele não pode divulgar esses dados, mesmo aos seus superiores.

Onde está a actividade? Uma actividade de aprendizagem significa que o estudante deve fazer algo para aprender, a simples leitura de um texto não é uma actividade de aprendizagem.

Resumo da Unidade

Na unidade de Serviços de redes vimos serviços essenciais de suporte à rede de computadores. Estes diferem dos serviços normais utilizados pelo utilizadores finais, isto é, as aplicações em que eles são acessados diretamente pelos utilizadores finais. Nesta unidade abordamos tópicos relacionadas com: serviço de configuração dinâmica dos endereços IP

(DHCP) , serviços de tradução de nomes (DNS), serviço de correios electrónicos, servidor de ficheiros e servidores de impressão.

Avaliação da Unidade

Verifique a sua compreensão!

Instruções

Estes exercícios permitiram verificar o estado dos conhecimentos dos alunos em relação da unidade de modelo de referencia.

Critérios de Avaliação

A avaliação deverá processar-se de uma forma contínua, sistemática e periódica. O tipo de avaliação corresponderá aos objectivos definidos na unidade.

Unidade 2. Serviços De Rede

Introdução à Unidade

Serviços de redes fornecem serviços essenciais de suporte a rede de computadores. Estes diferem dos serviços normais utilizados pelo utilizadores finais, isto é, as aplicações em que eles são acessados diretamente pelos utilizadores finais. Em vez disso, esses serviços são usados por computadores em rede para simplificar algumas actividades por exemplo, instalação, configuração e operacionalização da própria rede. Nesta unidade abordaremos tópicos relacionadas com: serviço de configuração dinâmica dos endereços IP (DHCP) , serviços de tradução de nomes (DNS), serviço de correios electrónicos, servidor de ficheiros e servidores de impressão.

Objetivos da Unidade

Após a conclusão desta unidade, deverá ser capaz de:

- Identificar um serviço de rede
- Descrever as funções e serviços de uma rede ponto a ponto e cliente/servidor
- Identificar e usar aplicações disponíveis
- Utilizar correctamente os serviços oferecidos pela rede

Termos-chave

Cliente: Este é um dispositivo de hardware ou software que acessa serviços disponibilizados por uma máquina centralizada ao qual ele se conecta.

servidor é um sistema de computação centralizada que fornece serviços a uma rede de computador.

Serviço: Esta é uma acção activada em uma máquina para ser consumida por uma outra ou por ele próprio na rede, de modo a servir o pedido do utilizador.

Actividades de Aprendizagem

Actividade 2.1 - Network Address Translation

a. Introdução

Os números IPs da Internet são finitos e cada número deve ser único. O crescimento explosivo da Internet tem transformado estes números em um recurso escasso, e para se obter um número ou conjunto de IPs válidos é necessário requisitá-los a um órgão regulador e pagar por eles. Logo, em muitos casos não se justifica construir redes locais utilizando-se números IPs válidos.

Como alternativa, certos intervalos de números IPs são considerados inválidos, isto é, não são utilizados na Internet, permitindo assim que eles possam ser utilizados em intranets sem problemas, ou seja, várias intranets podem utilizá-los desde que não estejam diretamente conectadas umas às outras. No entanto, isso cria um dilema: como conectar uma intranet que utiliza números IPs inválidos à Internet?

A resposta a essa pergunta é através da utilização de um roteador que possua um número IP válido e que seja capaz de fazer uma tradução de endereços de rede (NAT).

b. Rede privada

A Rede IP privada é uma rede IP que não está directamente ligado à internet. Endereços IP na rede privada pode ser atribuídos arbitráriamente sem uma garantia de serem globalmente únicos. Geralmente, as redes privadas usam endereços a partir do seguinte intervalo de endereços.

Na figura abaixo está um diagrama mostrando uma rede privada:

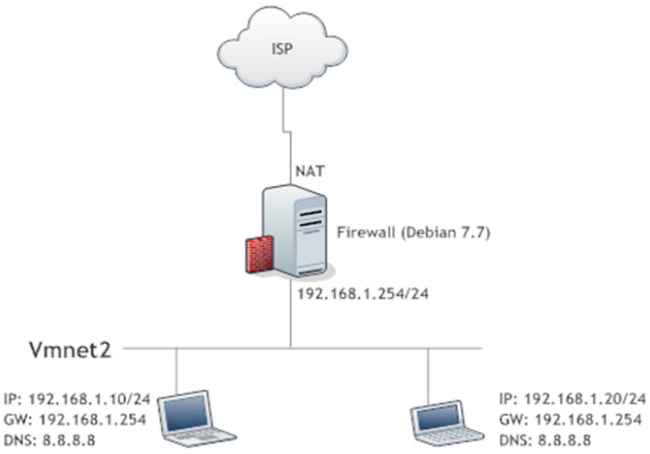


Figura 1. Mostra uma rede privada ligada à Internet

2.1.2 Rede pública

Uma rede pública é um tipo de rede em que qualquer um, ou seja, o público em geral, tem acesso e através dela pode se conectar a outras redes ou à Internet. Para a rede pública existir, os dispositivos conectados devem ser fornecidos com o endereço IP público, onde cada endereço IP utilizado é globalmente exclusivo.

2.1.2 Operação básica do NAT

O diagrama abaixo mostra o funcionamento básico do DNAT e SNAT.

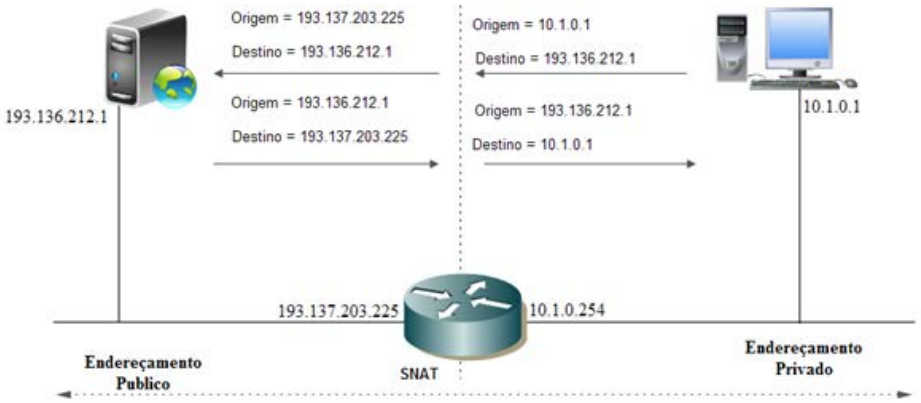


Figura 2. Mostra o processo de tradução do endereço

ONDE ESTÁ A ACTIVIDADE?

Actividades de Aprendizagem

Actividade 2.2 - Dynamic Host Configuration protocol

a. Introdução

Dynamic Host Configuration Protocol (DHCP) é um protocolo de comunicação que permitem aos administradores de rede gerenciar centralmente e automatizar a atribuição de endereços IP em uma rede. Em uma rede IP, cada dispositivo conectado à Internet precisa de um endereço IP único. DHCP permite a um administrador de rede supervisionar e distribuir endereços IP a partir de um ponto central e enviar automaticamente um novo endereço IP quando um computador estiver conectado a um lugar diferente na rede.

DHCP usa o conceito de "leasing" ou a quantidade de tempo que um determinado endereço IP será válido por um computador. DHCP suporta endereços estáticos para servidores de modo que não sejam atribuidos endereços IP de forma aleatória.

b. Funcionamento do DHCP

O cliente transmite uma mensagem DHCPDISCOVER para todos os servidores DHCP na rede. A mensagem DHCPDISCOVER pode incluir algumas opções, como sugestão de endereço IP ou a duração da oferta do IP.

Cada servidor DHCP pode responder ao cliente com uma mensagem DHCPOFFER que inclui um endereço de IP disponível e outras opções de configuração. Os servidores registram o endereço como oferecido ao cliente para evitar que o mesmo endereço, que está sendo oferecido a outros clientes, em caso de novas mensagens DHCPDISCOVER, sejam recebidas antes do primeiro cliente tenha concluído a sua configuração.

O cliente receberá uma ou mais mensagens DHCPOFFER a partir de um ou mais servidores. Neste caso, o cliente escolhe um com base nos parâmetros de configuração oferecidos e transmite uma mensagem DHCPREQUEST que inclui a opção identificador do servidor para

indicar qual a mensagem que seleccionou e a opção endereço de IP solicitado, retirado o seu endereço IP da oferta seleccionada. No caso em que não há ofertas recebidas e se o cliente tiver conhecimento de um endereço de rede anterior, o cliente pode reutilizar esse endereço, se o seu contrato ainda for válido, até o contrato expirar.

Os servidores recebem a mensagem DHCPREQUEST a partir do cliente mas apenas um DHCP responde à mensagem DHCPREQUEST e outros ignoram. O servidor lecionado responde uma mensagem DHCPNACK contendo os parâmetros de configuração para o cliente solicitante.

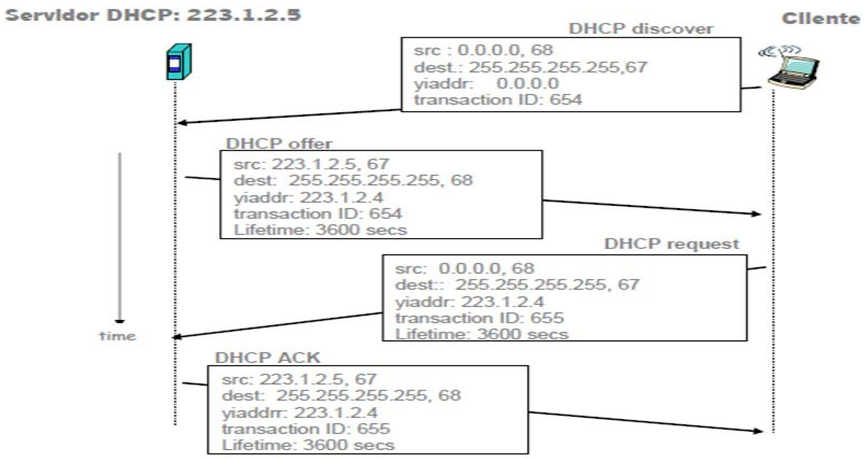


Figura 3. Mostra de troca de mensagens DHCP

Onde está a actividade de aprendizagem?

Actividades de Aprendizagem

Actividade 2.3 - Domain Name System (Sistema de Nomes de Domínio)

a. Introdução

Os seres humanos, podem ser identificados por diversas maneiras. Por exemplo, podemos ser identificados pelo nome que aparece no bilhete de identidade, passaporte ou NUIT. Também poderemos ser identificados pelo número desses documentos e embora cada um desses números possa ser usado para identificar pessoas, em um dado contexto um pode ser mais adequado que outro. Assim como seres humanos podem ser identificados de várias maneiras, exatamente o mesmo acontece com os host's na Internet. Os nomes como www.up.ac.mz, cnn.com, www.yahoo.com, gaia.cs.umass.edu e cis.poly.edu - são fáceis de lembrar e, portanto, apreciados pelos seres humanos.

Todavia, eles fornecem pouca informação sobre a localização de um host na Internet. (Um nome como www.eurecom.fr, que termina com o código do país .fr, nos informa que o host provavelmente está na França, mas não diz muito mais do que isso.)

Os nomes dos servidores podem consistir em caracteres alfanuméricos de comprimento variável mas seriam difíceis de ser processados por router's. Por essas razões, os host's também são identificados pelo endereços IP.

Um endereço IP é constituído por 4 bytes e sua estrutura hierárquica é rígida. Ele é semelhante a 121.7.106.83, no qual cada ponto separa um dos bytes expressos em notação decimal de 0 a 255. Um endereço IP é hierárquico porque, ao examiná-lo da esquerda para a direita, obtemos mais informações específicas sobre onde o host está localizado na Internet.

De maneira semelhante, quando examinamos um endereço postal de cima para baixo, obtemos informações cada vez mais específicas sobre a localização do destinatário.

Acabamos de ver que há duas maneiras de identificar um host - por um nome e um endereço IP do Host.

b. The Internet's Directory Service (O Sistema de Directório da Internet)

As pessoas preferem o identificador por nome de host por ser mais fácil de lembrar, ao passo que router's preferem endereços IP. Para satisfazer essas preferência, é necessário um serviço de directório que traduza nomes de host's para endereços IP. Esta é a tarefa principal do DNS (domain name system - sistema de nomes de domínio) da Internet.

O que é DNS ? - i) é uma base de dados distribuído implementado em uma hierarquia de servidores de nome (servidores DNS), e 2) um protocolo de camada de aplicação que permite que host's consultem a base de dados distribuído.

O que acontece quando um utilizador, requisita o URL www.someschool.edu/index.html?

Para que a máquina do utilizador possa enviar uma mensagem de requisição HTTP ao servidor Web www.someschool.edu, ela precisa primeiro obter o endereço IP de www.someschool.edu. Isso é feito da seguinte maneira:

- A máquina do utilizador executa o lado cliente da aplicação DNS
- O browser extrai o nome de host, www.someschool.edu, do URL
- passa o nome para o lado cliente da aplicação DNS.
- O cliente DNS envia uma consulta contendo o nome do host para um servidor DNS
- O cliente DNS finalmente recebe uma resposta, que inclui o endereço IP correspondente ao nome do servidor
- Logo o browser receba o endereço do DNS, pode abrir uma conexão TCP com o processo servidor HTTP localizado naquele endereço IP.

c. Base de dados distribuida e hierárquica

DNS usa um grande número de servidores, organizados de maneira hierárquica e distribuídos por todo o mundo. Nenhum servidor de nomes isolado tem todos os mapeamentos para todos os hostname da Internet.

Há três classes de servidores de nomes: servidores de nomes raiz, servidores DNS de domínio de alto nível (top-level domain - TLD) e servidores DNS com autoridade - organizados em uma hierarquia.

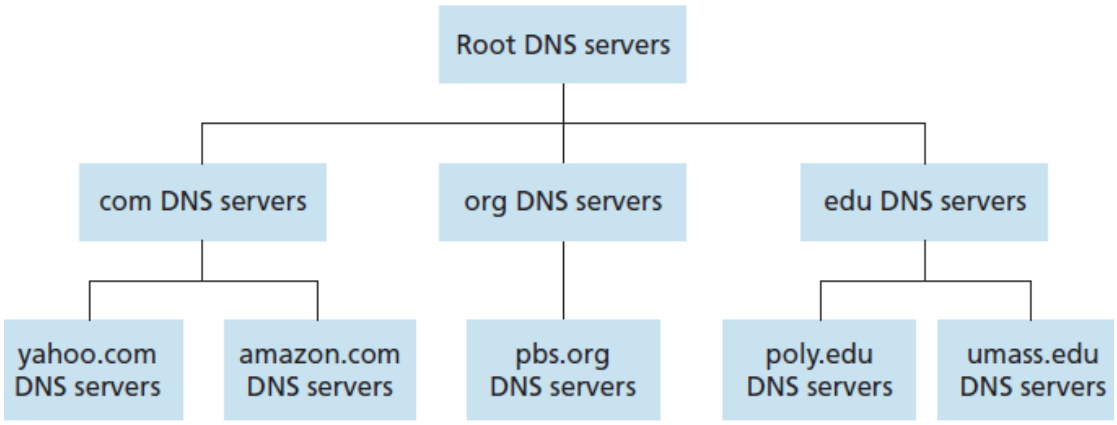


Figura 4. Base de dados distribuída e hierárquica

Na Internet há 13 servidores de nomes raiz (denominados de A a M) e a maior parte deles está localizada na América do Norte...!!!

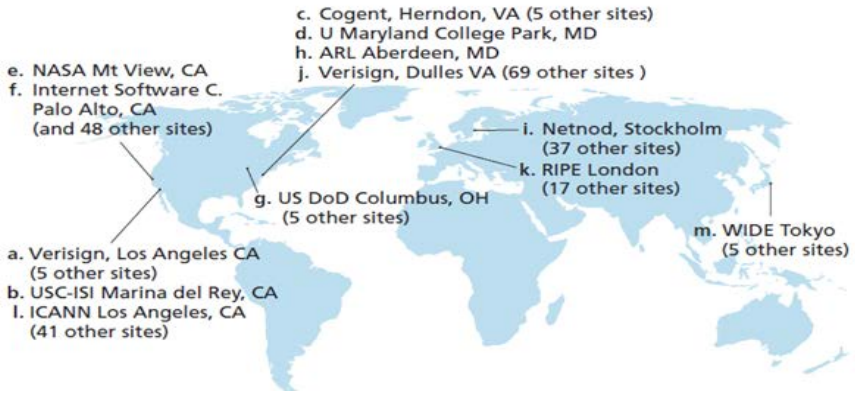


Figura 5. Os13 servidores de nomes raiz

d. Funcionamento do Domain Name System

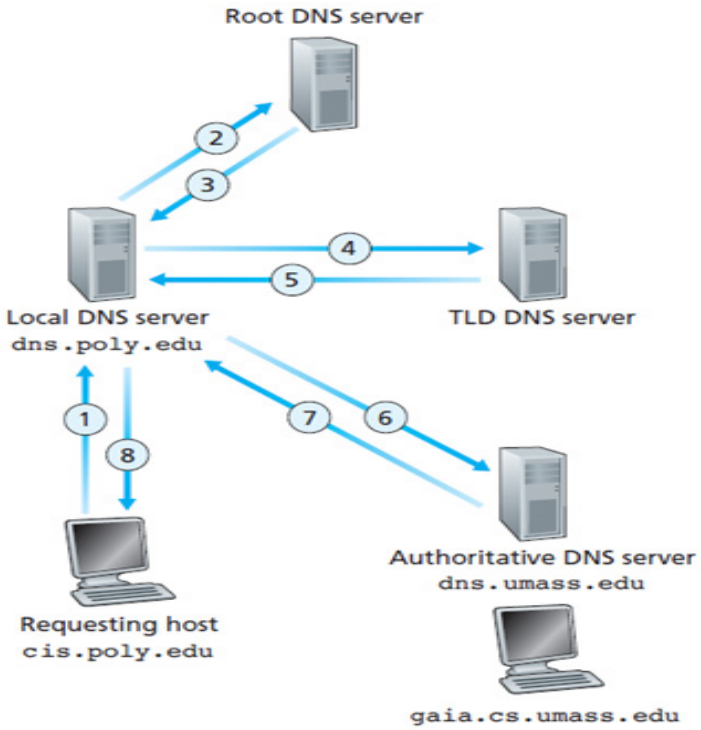
O DNS é utilizado por outras entidades da camada de aplicação, por exemplo: HTTP, SMTP e FTP - para traduzir nomes de servidores fornecidos por utilizadores para endereços IP.

O Host cis.poly.edu pretende o endereço IP de gaia.cs.umass.edu

Modo interactivo:

Servidor contactado responde com o nome do servidor a contactar

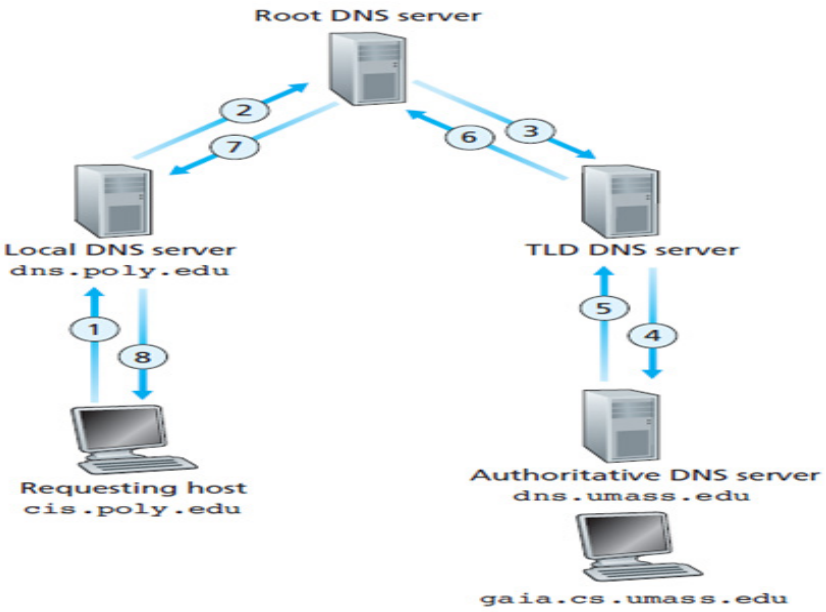
"Eu não conheço esse nome, mas pergunte a este servidor".



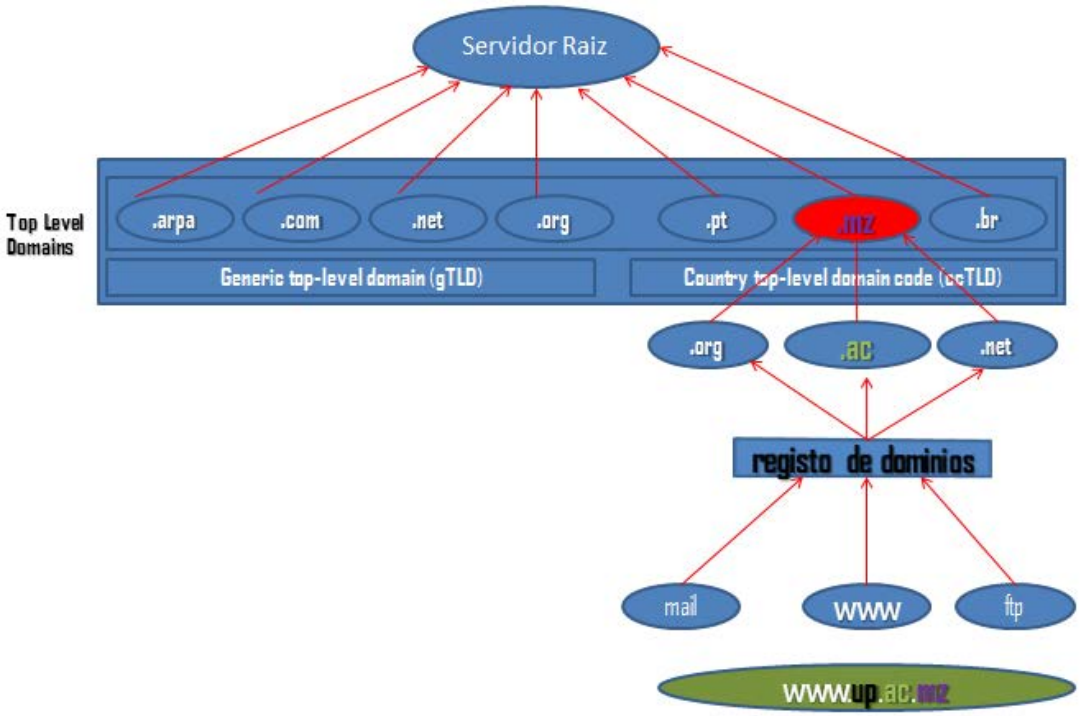
Modo recursivo:

Coloca o fardo da resolução no servidor de nomes contactado

Fardo pesado?



e. Estrutura do domínio de nome



Actividades de Aprendizagem

Actividade 2.4 - Servidor Web

a. Introdução

Até a decada 90, a Internet, era usada primordialmente por pesquisadores, acadêmicos e estudantes universitários para se interligar com servidores remotos transferir ficheiros, enviar e receber correio electrónico. Embora essas aplicações fossem (e continuem a ser) extremamente úteis, a Internet não era conhecida fora das comunidades acadêmicas e de pesquisa.

Um servidor web é um computador com software especial para hospedar páginas web e aplicações web. Este é o computador que fornece serviços Web para utilizadores de intranet ou Internet. O servidor web hospeda as páginas, scripts, programas e arquivos multimídia e serve-os usando o protocolo HTTP. Uma série de tecnologias do lado do servidor podem ser usadas para aumentar o poder do servidor para além da sua capacidade de entregar páginas (por exemplo, páginas HTML, páginas JSP)

b. Descrição geral do HTTP

O HTTP - Protocolo de Transferência de Hipertexto (HyperText Transfer Protocol) - protocolo de camada de aplicação da Web, está no coração da Web e é definido no [RFC 1945] e no [RFC 2616]. O HTTP é implementado em dois programas: um programa cliente e outro servidor. Os dois programas, executados em sistemas finais diferentes, conversam um com o

outro por meio da troca de mensagens HTTP. O HTTP define a estrutura dessas mensagens e o modo como o cliente e o servidor as trocam. Antes de explicarmos detalhadamente o HTTP, devemos rever a terminologia da Web. Uma página Web (também denominada documento) é constituída de objetos. Um objeto é simplesmente um arquivo - tal como um arquivo HTML, uma imagem JPEG, um applet Java, ou um clipe de vídeo — que se pode acessar com um único URL. A maioria das páginas Web é constituída de um arquivo-base HTML e diversos objetos referenciados. Por exemplo, se uma página Web contiver um texto HTML e cinco imagens JPEG, então ela terá seis objetos: o arquivo-base HTML e mais as cinco imagens. O arquivo-base HTML referencia os outros objetos na página com os URLs dos objetos. Cada URL tem dois componentes: o nome do hospedeiro do servidor que abriga o objeto e o nome do caminho do objeto. Por exemplo, no URL http://www.someSchool.edu/someDepartment/picture.gif.

O HTTP usa o TCP na camada de transporte em vez de rodar em UDP. O cliente HTTP primeiramente inicia uma conexão TCP com o servidor.

c. Funcionamento do protocolo HTTP

O cliente envia mensagens de requisição HTTP para sua interface socket e recebe mensagens de resposta HTTP de sua interface socket. De maneira semelhante, o servidor HTTP recebe mensagens de requisição de sua interface socket e envia mensagens de resposta para sua interface socket. Assim que o cliente envia uma mensagem para sua interface socket, a mensagem sai de suas mãos e "passa para as mãos do TCP". TCP provê ao HTTP um serviço confiável de transferência de dados, o que implica que toda mensagem de requisição HTTP emitida por um processo cliente chegará intacta ao servidor. De maneira semelhante, toda mensagem de resposta HTTP emitida pelo processo servidor chegará intacta ao cliente.

Figura 6: Mostra troca de mensagens HTTP

d. Conexões persistentes e não persistentes

Em muitas aplicações da Internet, o cliente e o servidor se comunicam por um período prolongado de tempo, em que o cliente faz uma série de requisições e o servidor responde a cada uma delas. Dependendo da aplicação e de como ela está sendo usada, a série de requisições pode ser feita de forma consecutiva, periodicamente em intervalos regulares ou esporadicamente. Quando a interação cliente-servidor acontece por meio de conexão TCP, o criador da aplicação precisa tomar uma importante decisão — cada par de requisição/resposta deve ser enviado por uma conexão TCP distinta ou todas as requisições e suas respostas devem ser enviadas por uma mesma conexão TCP? Na abordagem anterior, a aplicação utiliza conexões não persistentes; e na última abordagem, conexões persistentes.

i. Conexões não persistentes

- Vamos analisar uma transferência de uma página Web de um servidor para um cliente em conexões não persistentes. Vamos supor que uma página consista em um arquivo-base HTML e em dez imagens JPEG e que todos esses 11 objetos residam no mesmo servidor. Suponha também que o URL para o arquivo-base HTTP seja http://www.someSchool.edu/someDepartment/home.index

O processo cliente HTTP inicia uma conexão TCP para o servidor www.someSchool.edu na porta número 80, que é o número de porta default para o HTTP. Associados à conexão TCP, haverá um socket no cliente e um socket no servidor.

O cliente HTTP envia uma mensagem de requisição HTTP ao servidor através de seu socket. Essa mensagem inclui o nome de caminho /someDepartment/home.index. (Discutiremos mensagens HTTP mais detalhadamente logo adiante.)

O processo servidor HTTP recebe a mensagem de requisição através de seu socket, extrai o objeto /someDepartment/home.index de seu armazenamento (RAM ou disco), encapsula o objeto em uma mensagem de resposta HTTP e a envia ao cliente através de seu socket.

O processo servidor HTTP ordena ao TCP que encerre a conexão TCP. (Mas, na realidade, o TCP só encerrará a conexão quando tiver certeza de que o cliente recebeu a mensagem de resposta intacta.)

O cliente HTTP recebe a mensagem de resposta e a conexão TCP é encerrada. A mensagem indica que o objeto encapsulado é um arquivo HTML. O cliente extrai o arquivo da mensagem de resposta, analisa o arquivo HTML e encontra referências aos dez objetos JPEG.

As primeiras quatro etapas são repetidas para cada um dos objetos JPEG referenciados.

Conexões não persistentes têm algumas desvantagens. Em primeiro lugar, uma nova conexão deve ser estabelecida e mantida para cada objeto solicitado. Para cada uma dessas conexões, devem ser alocados buffers TCP e conservadas variáveis TCP tanto no cliente quanto no servidor.

Isso pode sobrecarregar seriamente o servidor Web, que poderá estar processando requisições de centenas de diferentes clientes ao mesmo tempo. Em segundo lugar, como acabamos de descrever, cada objeto sofre dois RTTs — um RTT para estabelecer a conexão TCP e um RTT para solicitar e receber um objeto.

ii. Conexões persistentes

- Em conexões persistentes, o servidor deixa a conexão TCP aberta após enviar resposta. Requisições e respostas subsequentes entre os mesmos cliente e servidor podem ser enviadas por meio da mesma conexão. Em particular, uma página Web inteira (no exemplo anterior, o arquivo-base HTML e as dez imagens) pode ser enviada mediante uma única conexão TCP persistente.

e.Formato da mensagem HTTP

As especificações do HTTP [RFC 2616] definem os formatos das mensagens HTTP. Há dois tipos de mensagens HTTP: de requisição e de resposta. apresentamos em seguida:

i. Mensagem de requisição HTTP

Apresentamos a seguir uma mensagem de requisição HTTP típica:

GET /somedir/page.html HTTP/1.1

Host: www.someschool.edu

Connection: close

User-agent: Mozilla/4.0

Accept-language: pt

ii. Mensagem de resposta HTTP

Apresentamos a seguir uma mensagem de resposta HTTP típica. Essa mensagem poderia ser a resposta ao exemplo de mensagem de requisição que acabamos de ver:

HTTP/1.1 200 OK

Connection: close

Date: Sat, 07 Jul 2007 12:00:15 GMT

Server: Apache/1.3.0 (Unix)

Last-Modified: Sun, 6 May 2007 09:23:24 GMT

Content-Length: 6821 Content-Type: text/html

(data data data data data ...)

Onde está a Actividade 2.4?

Actividades de Aprendizagem

Actividade 2.5 - Correio eletrônico

a. Introdução

O correio eletrônico (eletronic mail ou e-mail) existe desde o início da Internet. É uma das aplicações mais importantes e de maior uso da Internet. Tal como o correio normal, o e-mail é um meio de comunicação assíncrono — as pessoas enviam e recebem mensagens quando for conveniente para elas, sem ter de estar coordenadas com o horário das outras pessoas. Ao contrário do correio normal, que anda a passos lentos, o correio eletrônico é rápido, fácil de distribuir e barato. O correio eletrônico moderno tem muitas características poderosas. Utilizando listas de mala direta, é possível enviar mensagens de e-mail, desejadas e indesejadas, a milhares de destinatários ao mesmo tempo. As mensagens do correio eletrônico moderno muitas vezes incluem anexos, hyperlinks, textos formatados em HTML e fotografias.

b. Funcionamento do correio electronico

A Figura abaixo apresenta uma visão do sistema de correio da Internet utilizando uma analogia com a correspondência por correio. Vemos, por esse diagrama, que há três componentes principais: agentes de utilizador, servidores de correio e o SMTP.

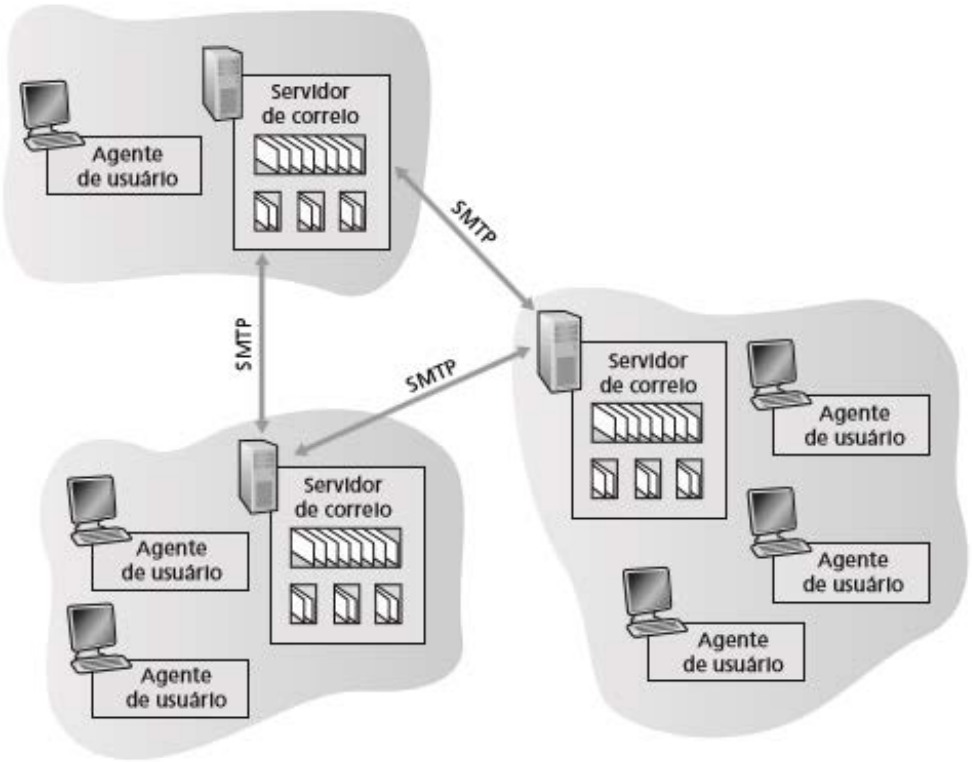


Figura 7: A troca de mensagens SMTP

Descreveremos agora cada um desses componentes partindo do seguinte contexto: um remetente, Alice, está enviando uma mensagem de e-mail para um destinatário, Bob. Agentes de usuários permitem que usuários leiam, respondam, retransmitam, salvem e componham mensagens. (Às vezes, agentes de usuário de correio eletrônico são denominados leitores de correio, mas, neste livro, evitaremos essa expressão.) Quando Alice termina de compôr sua mensagem, seu agente de utilizador a envia a seu servidor de correio, onde ela é colocada na fila de saída de mensagens desse servidor. Quando Bob quer ler uma mensagem, seu agente de utilizador a extrai da caixa de correio em seu servidor de correio.

c. Protocolo SMTP

O SMTP, definido no RFC 5321, está no coração do correio eletrônico da Internet. esse protocolo transfere mensagens de servidores de correio remetentes para servidores de correio destinatários. O SMTP é muito mais antigo que o HTTP. Para ilustrar essa operação básica do SMTP, vamos percorrer um cenário comum. Suponha que Alice queira enviar a Bob uma simples mensagem:

1. Alice chama seu agente de usuário para e-mail, fornece o endereço de Bob (por exemplo, bob@someschool.edu), compõe uma mensagem e instrui o agente de usuário a enviar a mensagem.

2. O agente de usuário de Alice envia a mensagem para seu servidor de correio, onde ela é colocada em uma fila de mensagens.

3. O lado cliente do SMTP, que funciona no servidor de correio de Alice, vê a mensagem na fila e abre uma conexão TCP para um servidor SMTP, que funciona no servidor de correio de Bob.

4. Após alguns procedimentos iniciais de apresentação, o cliente SMTP envia a mensagem de Alice para dentro da conexão TCP.

5. No servidor de correio de Bob, o lado servidor do SMTP recebe a mensagem e a coloca na caixa postal dele.

6. Bob chama seu agente de usuário para ler a mensagem quando for mais conveniente para ele.

Esse cenário está resumido na figura abaixo:

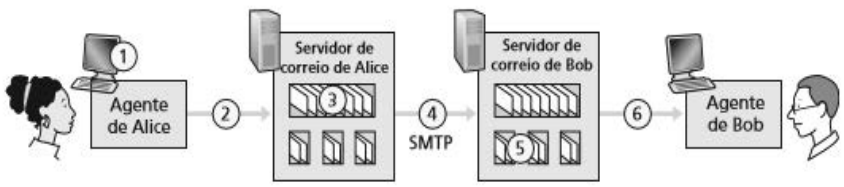


Figura 8: Troca de mensagens SMTP

d. Protocolos de acesso ao correio

Quando o SMTP entrega a mensagem do servidor de correio de Alice ao servidor de correio de Bob, ela é colocada na caixa postal de Bob. Durante toda essa discussão, ficou tacitamente subentendido que Bob lê sua correspondência ao entrar no hospedeiro servidor e, em seguida, executa o leitor de correio que roda naquela máquina. Até o início da década de 1990, este era o modo padronizado de acessar o correio. Mas hoje o acesso ao correio usa uma arquitectura cliente–servidor — o usuário típico lê e-mails com um cliente que funciona em seu sistema final, por exemplo, um PC no escritório, um laptop ou um PDA. Quando executam um cliente de correio em PC local, usuários desfrutam de uma série de propriedades, inclusive a capacidade de ver mensagens e anexos multimídia.

De que forma um destinatário como Bob, que executa um agente de utilizador em seu PC local, obtém suas mensagens que estão em um servidor de correio dentro do seu ISP? Note que o agente de usuário de Bob não pode usar SMTP para obter as mensagens porque essa operação é de recuperação (pull), e o SMTP é um protocolo de envio (push). O quebra-cabeça é concluído com a introdução de um protocolo especial de acesso ao correio que transfere mensagens do servidor de correio de Bob para seu PC local. Atualmente, há vários protocolos populares de acesso a correio, entre eles POP3 (Post Office Protocol versão 3), IMAP (Internet Mail Access Protocol) e HTTP.

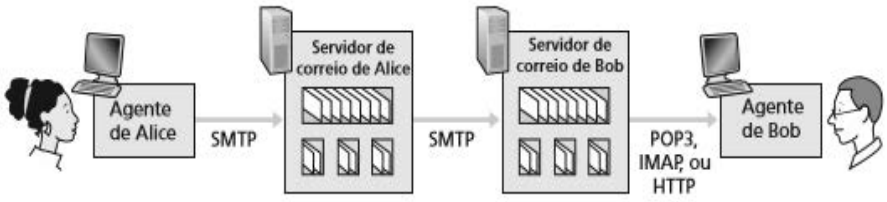


Figura 7: Agente SMTP, POP, IMAP ou HTTP

e. E-mail pela Web

Hoje, um número cada vez maior de usuários está enviando e acessando e-mails por meio de seus browsers Web. O Hotmail lançou o e-mail com acesso pela Web em meados da década de 1990; agora, esse tipo de acesso é fornecido por praticamente todos os sites ISP, bem como universidades e empresas importantes. Com esse serviço, o agente de usuário é um browser Web comum e o usuário se comunica com sua caixa postal remota via HTTP. Quando um destinatário, por exemplo, Bob, quer acessar uma mensagem em sua caixa postal, ela é enviada do servidor de correio para o browser de Bob usando o protocolo HTTP, e não os protocolos POP3 ou IMAP.

Onde está a Actividade de Aprendizagem??

Actividades de Aprendizagem

Actividade 2.6 - Transferência de arquivo

a. ntrodução

Em uma sessão FTP típica, o usuário, sentado à frente de um servidor local, quer transferir arquivos de ou para um hospedeiro remoto. Para acessar a conta remota, o usuário deve fornecer uma identificação e uma senha. Após fornecer essas informações de autorização, pode transferir arquivos do sistema local de arquivos para o sistema remoto e vice-versa.

A figura abaixo mostra, como o utilizador interage com o FTP por meio de um agente de utilizador FTP. Em primeiro lugar, ele fornece o nome do servidor remoto, o que faz com que o processo cliente FTP do servidor local estabeleça uma conexão TCP com o processo servidor FTP do hospedeiro remoto. O utilizador então fornece sua identificação e senha, que são enviadas pela conexão TCP como parte dos comandos FTP. Assim que autorizado pelo servidor, o usuário copia um ou mais arquivos armazenados no sistema de arquivo local para o sistema de arquivo remoto (ou vice-versa).

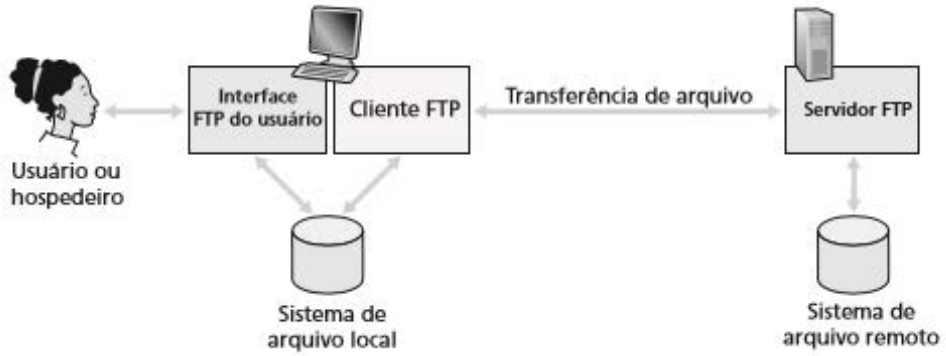


Figura 9: A troca de mensagens FTP

Durante uma sessão, o servidor FTP deve manter informações de estado sobre o usuário. Em particular, o servidor deve associar a conexão de controle com uma conta de usuário específica e também deve monitorar o diretório corrente do usuário enquanto este passeia pela árvore do diretório remoto. Monitorar essas informações de estado para cada sessão de usuário em curso limita significativamente o número total de sessões que o FTP pode manter simultaneamente. Lembre-se de que o HTTP, por outro lado, é sem estado — não tem de monitorar o estado de nenhum utilizador.

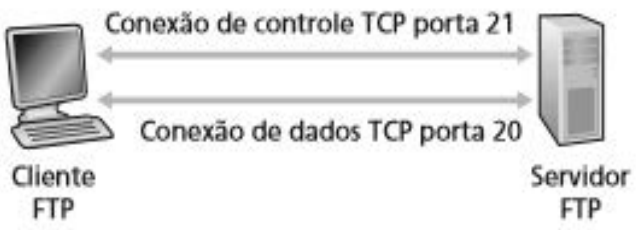


Figura 10. ?????

b. Comandos e respostas FTP

Encerraremos esta unidade com uma breve discussão sobre alguns dos comandos mais comuns do FTP. Os comandos, do cliente para o servidor, e as respostas, do servidor para o cliente, são enviados por meio da conexão de controle no formato ASCII de 7 bits. Assim, tal como comandos HTTP, comandos FTP também podem ser lidos pelas pessoas. Para separar comandos sucessivos, um 'carriage return' e um 'line feed' encerram cada um deles. Cada comando é constituído de quatro caracteres ASCII maiúsculos, alguns com argumentos opcionais. Alguns dos comandos mais comuns são descritos a seguir:

- USER username: usado para enviar identificação do utilizador ao servidor.
- PASS password: usado para enviar a senha do utilizador ao servidor.
- LIST: usado para pedir ao servidor que envie uma lista com todos os arquivos existentes no actual diretório remoto. A lista de arquivos é enviada por meio de uma conexão de dados (nova e não persistente), e não pela conexão TCP de controle.
- RETR filename: usado para extrair (isto é, obter) um arquivo do diretório atual do hospedeiro remoto. Ativa o hospedeiro remoto para que abra uma conexão de dados e envie o arquivo requisitado por essa conexão.
- STOR filename: usado para armazenar (isto é, inserir) um arquivo no diretório atual do hospedeiro remoto.

Há, particularmente, uma correspondência unívoca entre o comando que o usuário gera e o comando FTP enviado pela conexão de controle. Cada comando é seguido de uma resposta, que é enviada do servidor ao cliente. As respostas são números de três dígitos com uma mensagem opcional após o número. Elas se assemelham, em estrutura, à codificação de estado e à frase da linha de estado da mensagem de resposta HTTP. Os inventores do HTTP incluíram intencionalmente essa similaridade nas mensagens de resposta HTTP. Algumas respostas típicas, junto com suas possíveis mensagens, são as seguintes:

331 Nome de usuário OK, senha requisitada

125 Conexão de dados já aberta; iniciando transferência

425 Não é possível abrir a conexão de dados

452 Erro ao escrever o arquivo

Actividades de Aprendizagem

Actividade 2.7 - File and Print Servers (Servidores de arquivo e de Impressão)

a. ntrodução

Os dois servidores de rede aqui discutidos serão: servidores de arquivo e impressão, tornar a rede mais conveniente para os usuários.

Não muito tempo atrás, unidades de disco e impressoras de alta qualidade eram relativamente caros. Hoje, cada sistema tem um disco rígido grande e muitos têm suas próprias impressoras de alta qualidade, mas isso nunca vai eliminar a necessidade de partilha de recursos. Servidores de arquivos permitem aos usuários armazenar arquivos importantes em um local central na rede a partir do qual é fácil adicionar segurança e para permitir que os usuários compartilhem arquivos. Um servidor de arquivo também tipicamente oferece um serviço de impressão, que fornece uma maneira fácil e conveniente de compartilhar impressoras.

b. File Sharing (Partilha de Arquivos))

O compartilhamento de arquivos não é o mesmo que a transferência de arquivos (a capacidade de mover um arquivo de um sistema para outro). Um verdadeiro sistema de compartilhamento de arquivos, não é necessário para mover arquivos inteiros em toda a rede. Ele permite que arquivos sejam acessados no nível de registro de modo que seja possível para um cliente ler um registro de um arquivo localizado em um servidor remoto, atualizar esse registro, e escrevê-lo de volta para o servidor - sem mover o arquivo completo do servidor para o cliente. Através de compartilhamento de arquivos, usuários e programas podem acessar arquivos localizados em sistemas remotos como se fossem arquivos locais. Em um ambiente de partilha de ficheiros perfeito, o usuário não conhece e nem se importa onde os arquivos são realmente armazenados. O administrador de rede terá que escolher o tipo de servidor de arquivo para realizar o compartilhamento de arquivos, muitas opções estão disponíveis, mas o NFS (para clientes Linux) e Samba (para clientes Windows) são os dois mais popular.

c. Printing Services (Serviço de Impressão)

Este é um serviço de rede útil que permite a partilha de impressoras, por todos, na rede. As vantagens de partilha de impressoras são como se segue:

São necessárias menos impressoras e menos dinheiro é gasto em impressoras e suprimentos.

Manutenção reduzida. Há menos máquinas para manter, e menos pessoas a passarem o tempo brincando com impressoras.

Acesso a impressoras especiais. Muito impressoras a cores de alta qualidade e muito impressoras de alta velocidade são caras e são necessárias apenas ocasionalmente. Compartilhando essas impressoras faz-se melhor uso dos recursos caros.

Resumo da Unidade

Na unidade de Serviços de redes vimos serviços essenciais de suporte a rede de computadores. Estes diferem dos serviços normais utilizados pelo utilizadores finais, isto é, as aplicações em que eles são acessados diretamente pelos utilizadores finais. nesta unidade abordamos tópicos relacionadas com: serviço de configuração dinâmica dos endereços IP (DHCP) , serviços de tradução de nomes (DNS), serviço de correios electrónicos, servidor de ficheiros e servidores de impressão.

Avaliação da Unidade

Verifique a sua compreensão!

Instruções

Estes exercícios permitiram verificar o estado dos conhecimentos dos alunos em relação da unidade de modelo de referencia.

Critérios de Avaliação

A avaliação deverá processar-se de uma forma contínua, sistemática e periódica. O tipo de avaliação corresponderá aos objectivos definidos na unidade.

Avaliação

1. Qual é a diferença entre um servidor e um sistema final ? Cite os tipos de sistemas finais. Um servidor Web é um sistema final?
2. A palavra protocolo é muito usada para descrever relações diplomáticas. Dê um exemplo de um protocolo diplomático
3. O que é um programa cliente? O que é um programa servidor? Um programa servidor requisita e recebe serviços de um programa cliente?
4. Que tipos de serviços de rede de computadores. estão disponíveis na sua faculdade ?

Leituras e outros Recursos

As leituras e outros recursos desta unidade encontram-se na lista de Leituras e Outros Recursos do curso.

Unidade 3. Ferramentas De Gestão De Redes

Introdução à Unidade

Os serviços fornecidos pelo redes devem apresentar um nível óptimo ou quase óptimo de qualidade pois caso contrário corre-se o risco da rede não ser utilizada e gerar grande frustração junto de utilizadores e administradores. O esforço de instalação bem como os gastos efectuados serão perdidos e a rede tornar-se-á inviável. E essencial dotar a quem? de ferramentas e mecanismos que permitam monitorar e corrigir situações anômalas que possam surgir durante a operação, de forma a aumentar o grau de confiança que o serviço apresenta face aos seus utilizadores.

Esta unidade é dedicada à apresentação dos principais conceitos relativos a medição e monitorização de redes de computadores. No final, destacam-se algumas ferramentas de monitorizações e controlo de redes tal como, Cacti, Nagios, NTOP e Dude.

Objetivos da Unidade

Após a conclusão desta unidade, deverá ser capaz de:

propor um conjunto de soluções que permitam melhorar o desempenho da rede.

Escolher e propor um conjunto de ferramentas de gestão de rede

analisar o tráfego e pacotes em redes de computadores

Monitorar e gerir a rede de computadores através do NMS

Termos-chave

Monitorização: consiste no controlo das actividades da rede de computadores através da medição do estado de várias parâmetros e equipamento

Gestão: A gestão consiste no conjunto de funções para controlar, planear, alocar, implementar, coordenar e monitorizar os recursos de rede.

Controlo: Esta categoria de gestão de desempenho consiste no controlo que permite fazer ajustes nos dispositivos de rede para melhorar o desempenho.

Métricas: As métricas estão relacionadas com parâmetros de rapidez, precisão, disponibilidade do sistema, taxa de erros e volume de trabalho produzido.

Actividades de Aprendizagem

Actividade 3.1 - Arquitecturas de Gestão

a. Introdução

A diversidade de opções tecnológicas para construir uma rede de dados, abriu caminho ao aumento de complexidade das tarefas de gestão, que vinham sendo efectuadas de um modo mais ou menos empírico e desorganizado. Nesta unidades são apresentadas as arquitecturas e mecanismos de gestão de redes de dados. Descrevem-se os passos para uma abordagem sistemática e as principais técnicas de avaliação são descritas e contextualizadas. No sentido de proceder à normalização de uma arquitectura genérica de gestão de redes, alguns organismos internacionais tem apresentado modelos e arquitecturas de gestão. A ISO (International Standards Organisation) desenvolveu, a partir da década 70, um grande esforço na tentativa de apresentar uma arquitectura de referência para redes de comunicação de dados. Deste trabalho resultou o modelo OSI (Open Systems Interconnection) ao qual foram posteriormente acrescentadas especificações para regulamentar os mecanismos de gestão e troca de informação de gestão.

Actualmente, as arquitecturas de gestão de redes estão fortemente polarizadas em torno de três soluções que serão discutidas nesta unidade: OSI (Open Systems Interconnection), INMF (Internet Network Management Framework) e TMN (Telecommunications Management Network).

b. Modelo de Gestão

A administração, ou gestão, de uma rede local á efectuada de forma a prever, identificar e corrigir falhas de funcionamento. As operações bâsicas efectuadas por um sistema deste tipo podem ser agrupadas em:

Recolha de informação de gestão.

Processamento de informação de gestão.

Realização de acções correctivas.

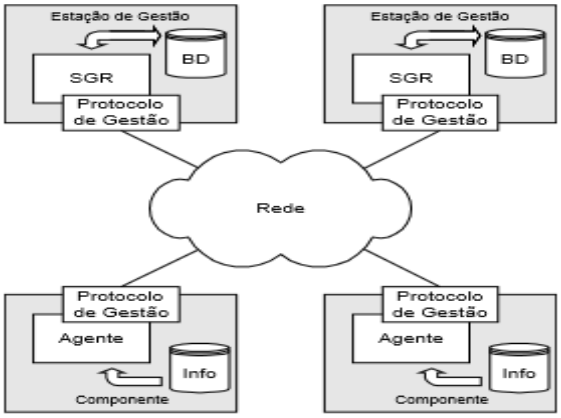


Figura 10: Modelo de gestão baseada em agente/Gestor

A troca de notificações e de comandos entre entidades de gestão é efectuada segundo um protocolo especifico, o protocolo de gestão. Por outro lado, a informação trocada representa vários parâmetros de funcionamento, relativos a uma entidade especifica, um conjunto de entidades ou própria infra-estrutura de comunicação. Este modelo simplificado à partilhado pelas três arquitecturas seguintes:

c. Arquitectura de gestão OSI

A ISO (International Standards Organisation), com a colaboração do ITU-T (International Telecommunications Union Telecommunication Standardisation Sector, ex-CCITT), desenvolveu um trabalho pioneiro na normalização de redes locais. Um dos resultados deste trabalho foi o modelo de referência de redes OSI (Open Systems Interconnection) [ISO 7498]. Este modelo consiste em cinco áreas funcionais:

Gestão de Falhas - agrupa os mecanismos que permitem detectar, isolar e corrigir funcionamentos anómalos.

Gestão de Contabilização - contêm mecanismos que permitem o estabelecimento de custos de utilização de recursos da rede.

Gestão de Configuração - mecanismos de controlo, identificação e consulta de dados necessários à operação dos dispositivos de ligação.

Gestão de Desempenho - mecanismos de avaliação de comportamento e de eficiência da comunicação.

Gestão de Segurança - segurança genérica dos sistemas de comunicação.

d. Arquitectura de gestão INMF

No entanto, a arquitectura INMF usa o protocolo de gestão de redes SNMP e este protocolo encontra-se neste momento na sua versão três (SNMPv3).

SNMPv1 é a versão padrão do protocolo SNMP, definida na RFC 1157. a ssgurança do SNMPv1 baseia-se em comunidades, que não são nada mais do que senha: string de texto puro que permite que qualquer aplicativo baseado em SNMP (que reconheça a string) tenha acesso a informações de gestão do dispositivo. Geralmente, existem três comunidades SNMPv1: Read-only, read-write e trap.

SNMPv2 é a segunda versão do protocolo SNMP. Esta versão possui melhorias em relação à primeira versão SNMPv1 incluindo operações adicionais, melhoria de desempenho, definições de segurança e comunicação entre NMS.

SNMPv3 diferencia-se das outras versões do SNMP no que diz respeito a três importantes serviços: autenticação, privacidade e controle de acesso. Para que esses serviços possam ser utilizados pelo SNMPv3 de forma organizada e eficiente, o software agente permite a criação de políticas de segurança que são utilizadas na autenticação, privacidade e controle de acesso. O SNMPv3 é composto por módulos, e cada entidade tem um mecanismo SNMP. Este mecanismo implementa diversas funções, por exemplo: envio de mensagens, controle de acesso a objectos, autenticação e criptografia de mensagens.

As comunidades no SNMP permitem definir confiabilidade entre NMS e os agentes. Um agente é configurado com três nomes de comunidade: read-only, read-write e trap. Os nomes de comunidade são basicamente como palavras-chave para restringir alguns tipos de operações.

A maioria dos equipamentos com suporte SNMP está configurada com strings de comunidade default, geralmente public para a comunidade read-only e private para a comunidade read-write.

e. Arquitectura de Gestão TMN

A Telecommunication managemeent Network - TMN providencia operações e mecanismos de gestão para redes de telecomunicações. Em particular, o sistema foi desenvolvido de forma a realizar o controlo e monitorização de redes de telecomunicações, incluindo funções de monitorização de falhas, análise de desempenho, controlo de encaminhamento e de configuração, taxação e controlo de acesso a TMN. Pode ser vista como uma rede paralela à rede da operadora, em perfeita concordância com esta, por intermédio de um conjunto de pontos de acesso normalizados (Figura 11).

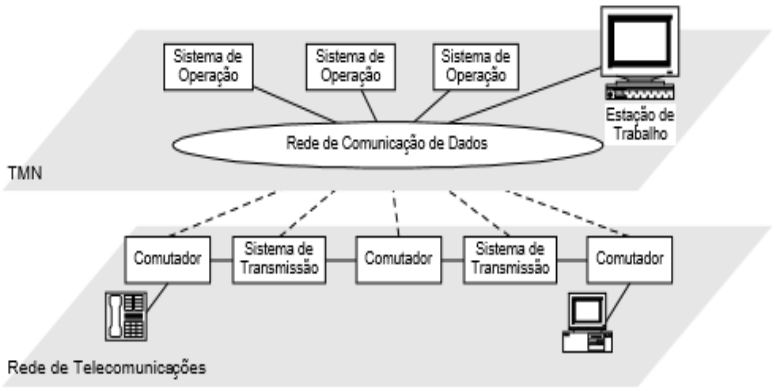


Figura 11: Modelo de gestão TMN

O processo de normalização do TMN teve inicio em 1985 pelo grupo de estudo do CCITT. Esta arquitectura apresenta três arquitecturas distintas [Cohen94]:

Arquitectura Funcional - descreve os blocos funcionais e os pontos de acesso aos blocos funcionais.

Arquitectura Física - descreve as interfaces e os componentes fisicos de uma TMN.

Arquitectura de Informação - descreve a aplicação dos princípios de gestão OSI em TMN.

Actividade 3.2 - Gestão Baseada na WWW

a. Introdução

As redes locais são intrinsecamente heterogêneas. É comum a coexistência de componentes de diversos fabricantes, derivada da implementação de diversas soluções tecnológicas ou dos contínuos avanços tecnológicos. A gestão de uma rede deste tipo é normalmente efectuada com o auxilio de ferramentas proprietárias, produzidas pelo fabricante para cada componente. O administrador de uma rede deste tipo necessita utilizar toda uma panóplia de ferramentas, de acordo com a diversidade existente, ou adquirir uma solução de aspecto geral. Este tipo de ferramentas é geralmente caro e requer hardware poderoso, pelo que a sua aquisição não se encontra ao alcance das instituições mais modestas.

Os serviços baseados na WWW (World Wide Web), como resultado da sua crescente popularidade, apresentam uma interface bem conhecida (web browser). A vulgaridade dos chamados browsers e a tendência actual para a integração de múltiplos serviços possibilita a coexistência de vários tipos de informação, de uma forma local ou distribuida. Estas características tornam a tecnologia adequada para a integração de diversas soluções de gestão normalizadas ou proprietárias. A integração pode ser efectuada de várias formas, não exclusivas:

- Pela definição de um esquema de equivalência entre o HyperText Transfer Protocol (HTTP) [RFC 1945] e o(s) protocolo (s) de gestão respectivo(s).
- Utilizando linguagens de programação interpretadas, do tipo Java, no desenvolvimento de aplicações de gestão.
- Pela extensão da tecnologia de WWW de modo a suportar operações de gestão.
- Utilizando a arquitectura CORBA (Common Object Request Broker) [Corba97] como núcleo de reunificação de diferentes soluções tecnológicas.

Onde está a actividade de aprendizagem?

Actividade 3.3 - Protocolos de gestão de Redes

a. Introdução

Os protocolos de gestão de redes são responsáveis por garantir a comunicação entre os recursos da rede que estão cada vez mais heterogêneas. Muitos protocolos de gestão foram especificados, dentre eles o CMIP (Common Management Information Protocol), o SGMP (Simple Gateway Management Protocol), o SNMP (Simple Network Management Protocol), e o RMON (Remote Network Monitoring). No entanto, o protocolo de gestão de redes SNMP foi o que mais se desenvolveu [3], pelo que será abordado com mais detalhe.

b. Simple Network Management Protocol - SNMP

Com o crescimento das redes de computadores, houve um custo e uma demanda muito grande de dispositivos cada vez mais complexos, tais como routers, switches e outros hosts, o que dificulta a gestão de todos estes dispositivos. Para suprir essa necessidade

foi desenvolvido o protocolo Simple Network Management Protocol, capaz de atender à necessidade cada vez maior de um padrão para gestão de dispositivos numa rede IP [3]. A arquitectura de gestão de redes baseada em SNMP é constituída pelos seguintes elementos:

- Network Management Station - NMS
  É um servidor que executa uma aplicação capaz de tratar tarefas de gestão de redes, como seja operações de polling a um agente e recepção de traps de agentes na rede.

- Agente
  É um software instalado e executado em dispositivos de uma rede, para que possam ser monitorizados pelo NMS.

- Polling
  No contexto de gestão de redes, significa consultar informações de um agente.

- Traps
  É um método utilizado por agentes para informar a NMS que algo aconteceu no dispositivo. A figura 12 mostra a troca de mensagem entre a NMS e um agente.

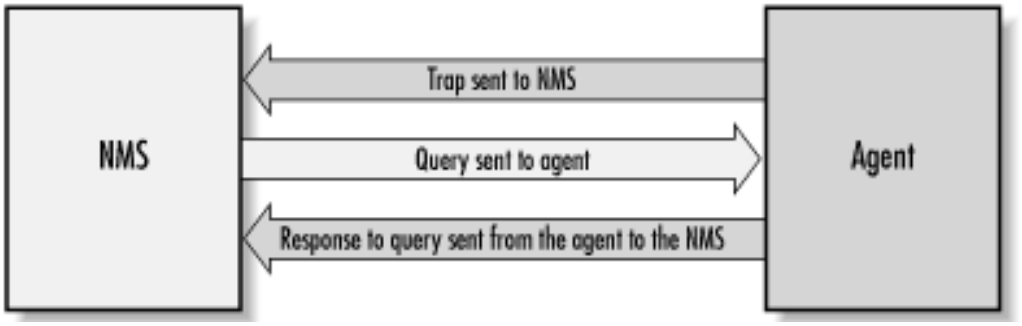


Figura 12: Troca de mensagem entre agente e Gestor

c. Modelo de Sistemas

Os modelos de sistemas podem ser classificados em físicos, modelos reais, tais como protótipos, que reproduzem o comportamento do sistema, e matemáticos, representados por fórmulas, algoritmos ou procedimentos que podem ser classificados nas seguintes categorias: analíticos, são fórmulas que definem, de forma exacta ou aproximada, o comportamento do sistema; simulados, em que algorítmos ou procedimentos representam o comportamento do sistema numa escala de tempo. A avaliação de desempenho requer um conhecimento íntimo do sistema a ser avaliado e uma escolha cuidadosa das metodologias, carga de trabalho, ferramentas de análise e técnicas de avaliação de desempenho e sua aplicabilidade.

Técnicas de Avaliação de Desempenho

Existe três técnicas de avaliação de desempenho, verificam-se as seguintes opções [2]: (i) medição; (ii) modelação analítica; e (iii) simulação. A modelação analítica e simulação podem ser utilizadas quando a medição não é possível por não existir um sistema real. Um outro aspecto importante a ter em conta é o

tempo disponível para a avaliação. Importa salientar que, quando o tempo para avaliação é curto a modelação analítica pode ser uma possível escolha, visto que a simulação e medição podem envolver um período longo. No entanto, a modelação analítica exige muitas simplificações e suposições. As simulações podem incorporar mais detalhes e requerem menos suposições.

Medição

Essa técnica de avaliação é aplicada quando o sistema em estudo existe e é acessível [7], por exemplo, um computador ou vários computadores e elementos de rede. O processo de medição começa quando um sistema é submetido a uma carga de trabalho e em seguida a ferramenta de monitorização recolhe os dados armazenados, calcula as métricas de desempenho, e exibe os resultados, por exemplo, através de gráficos.

Modelação Analítica

A modelação analítica consiste na criação de modelos matemáticos e equações que descrevem certos aspectos do sistema [7]. Para a modelação analítica de sistemas e redes de comunicação, muitas vezes são usados modelos probabilísticos para descrever a avaliação dos sistemas.

Simulação

A técnica de simulação baseia-se num programa de computador escrito numa linguagem de propósito geral ou numa linguagem especial orientada à simulação [7]. A simulação implementa os aspectos originais mais importantes, muitas vezes de uma forma abstracta e simplificada. No entanto, a vantagem da simulação sobre a modelação analítica é que ela permite um maior nível de detalhe e evita demasiadas simplificações.Na modelação analítica, o nível de detalhe é frequentemente limitado pela expressividade do método analítico, enquanto para simulação, é apenas limitada pela disponibilidade de tempo e recursos.

d. Critério de Selecção de Métricas de Desempenho

Para cada estudo de avaliação de desempenho, existe um conjunto de critérios de desempenho e métricas que devem ser escolhidos. Uma maneira de preparar este conjunto é listar os serviços oferecidos pelo sistema.

Existem vários resultados possíveis na execução dos serviços. Geralmente, estes resultados podem ser classificados em três categorias, o sistema pode executar o serviço correctamente, incorrectamente, ou não realizar o serviço. Se o sistema executa o serviço correctamente, o seu desempenho é medido pelo tempo necessário para executar o serviço, a taxa a que o serviço é realizado e os recursos consumidos durante a execução do serviço.

Estas três métricas relacionadas com time – rate – resource para o desempenho bem sucedido são chamados também de métricas de: tempo de resposta (responsiveness), produtividade (productivity) e utilização (utilization), respectivamente.

Se o sistema executa o serviço incorrectamente, diz-se que ocorreu um erro. É útil classificar os erros e determinar as probabilidades de cada classe de erros. Se o sistema não executa o serviço, ele é considerado indisponível. Mais uma vez, é útil classificar os modos de falha ou indisponibilidade e determinar as probabilidades de cada classe de erros.

As métricas associadas com os três resultados, ou seja, serviço de sucesso, erro e indisponibilidade, são também chamadas métricas de rapidez (speed), confiabilidade (reliability) e disponibilidade (availability).

e. Métricas de avaliação de desempenho

Conforme referido, é muito importante ter em mente quais são as métricas relevante a medir para se obter o resultado de análise desejado. Existem três métodos [8] que são usados para obter dados referentes a métricas na rede: consulta dos dispositivos da rede para obter informações armazenadas; observando o tráfego existente na rede para detectar sinais que afectam o desempenho da rede; e gerando tráfego de teste para enviar na rede para testar o desempenho da mesma. Descrevem-se de seguida as métricas que são objecto de estudo neste trabalho [9]:

Throughput

É definido como sendo a quantidade de dados que passa por um sistema durante certo intervalo de tempo [9]. Para sistemas interactivos, o throughput é medido em solicitações por segundo, para CPUs, o throughput é medido em milhões de instruções por segundo (mips), em redes de computadores, o throughput é medido em pacotes por segundo (pps) ou bits por segundo (bps) e para sistemas de processamento de transições, o throughput é medido em transições por segundo (tps).

Round Trip Time (RTT)

É o tempo que um pacote leva para atingir o outro host e voltar à origem [9]. Com esse valor obtêm-se o tempo em que um pacote demora para atravessar toda a rede e voltar à sua origem. Uma aproximação do atraso num sentido (Oney Way Delay) pode ser obtido calculando a metade do RTT, que representaria o tempo aproximado para o pacote atingir o destino [10]. A assimetria das rotas e carga dos sistemas envolvidos em cada um dos sentidos faz com que seja apenas uma aproximação. A tabela 3 mostra as características de desempenho de redes.

Perda de Pacotes

erda de Pacotes é o índice que mede a taxa de sucesso na transmissão de pacotes IP entre dois pontos da rede [9]. É normalmente expressa como uma percentagem, indicando o percentual de pacotes perdidos. Quanto menor a perda de pacotes, maior a eficiência da rede.

A perda de pacote é muitas vezes inevitável, e pode comprometer significativamente a qualidade do serviço prestado sobre o IP.

Utilização de Recursos

Quantidade de recursos consumidos, por exemplo, ciclos de CPU e uso de memória [9].

f. Metodologias de medição

O tráfego de rede vem sendo analisado desde o desenvolvimento da ARPANET, em que medições realizadas nas redes proporcionam informações úteis sobre o desempenho e características do tráfego que passam por elas. As metodologias de medição podem ser classificadas em duas categorias a saber [9]:

Medição Passiva

A medição passiva consiste em observar o tráfego que passa pelos pontos seleccionados dentro da rede. A análise dos dados colectados possibilita saber a utilização e características do tráfego. Este é um método não intrusivo, ou seja, a colecta de dados não afecta de forma significativa o tráfego que passa pela rede. A maioria das ferramentas de medição da rede enquadra-se nesta categoria.

Medição Activa

A medição activa emite tráfego na rede (tráfego de prova) e mede o seu

desempenho baseado no que foi emitido. Este tipo de medição é considerado intrusivo, e se não for bem controlado o tráfego gerado pode influenciar no funcionamento da rede e, consequentemente, nas próprias medições.

g. Ferramentas de monitorização

Uma ferramenta de monitorização é responsável por colectar os dados de desempenho dos sistemas, utilizando um protocolo de consulta (query protocol). Adicionalmente, analisa os dados para facilitar a interpretação dos resultados pelo administrador de rede [7]. Segundo Raj Jain [2] a classificação das ferramentas de monitorização mais comum é baseada em: software, hardware, firmware ou híbrida.

Ferramentas Baseadas em Software

Em geral, as ferramentas de monitorização baseada em software são muito menos dispendiosas do que as baseadas em hardware, mas não podem oferecer a mesma funcionalidade e desempenho de uma monitorização de tráfego de rede dedicada baseada em hardware [9] [7] [11] [12].

Ferramentas Baseadas em Hardware

As ferramentas baseadas em hardware envolvem equipamentos específicos, concebidos expressamente para a recolha e análise de dados da rede. Essas ferramentas muitas vezes são caras, dependendo do número de interfaces de rede, os tipos de placas de rede, a capacidade de armazenamento e as capacidades de análise de protocolos. Como não há recursos dos sistemas

que são consumidos na monitorização, as medições baseadas em hardware geralmente têm menor sobrecarga do que a medição baseada em software [9] [7] [11] [12].

Ferramentas Baseadas em Firmware

As ferramentas baseadas em firmware são implementadas modificando o microcódigo do processador. Essas ferramentas são úteis em aplicações onde as considerações de tempo impedem o uso de ferramentas baseadas em software e o ponto de colecta de dados dificulta a monitorização baseada em hardware. As ferramentas baseadas em firmware são utilizadas para monitorização de rede, onde as interfaces de rede existentes podem ser facilmente micro-programadas para monitorar todo o tráfego na rede.

Ferramentas Híbridas

Este tipo de ferramentas baseiam-se numa combinação de hardware, firmware ou software. Por exemplo, uma ferramenta híbrida composta pela componente de hardware de colecta de dados e por ferramentas baseadas em software pode permitir uma colecta de dados mais eficiente [2].

No contexto da medição passiva, dados colectados pelas ferramentas de medição podem ser obtidos através dos agentes de duas maneiras diferentes [5]:

consulta a dados num agente, através do protocolo de gestão de redes. Por exemplo, o SNMP é usado como o protocolo de consulta, o que corresponde à leitura de variáveis da MIB. No contexto de gestão de redes, significa polling.

o agente informa a NMS que algo aconteceu no dispositivo. No contexto de gestão de redes é conhecido por traps.

As ferramentas de medição podem suportar a colecta e análise de dados da rede nos seguintes modos [9] [7] [11] [12]:

Medição On-line

São ferramentas que suportam a colecta e análise de dados em tempo real, permitindo normalmente a visualização on-line de gráficos de tráfego. A maioria das ferramentas baseadas em hardware suporta esta funcionalidade.

Medição Off-line

Outras ferramentas têm o objectivo apenas de colectar e armazenar o tráfego de rede, sendo a análise realizada em um momento posterior ao estágio on-line. Isto é, a medição de rede destina-se apenas à recolha em tempo real e a análise de dados de tráfego é feita em off-line.

Quanto aos níveis protocolares abrangidos, as ferramentas de medição diferem no nível protocolar no qual os dados são colectados e a análise de tráfego é realizada. Muitas ferramentas de medição suportam a análise de protocolos multi-layer, isto é, recolhem e analisam tráfego aos vários níveis protocolares. [9][7] [11] [12].

As medições podem ser feitas em LANs ou WANs [9] [7] [11] [12]:

Medição em Local Area Network – LAN

Os primeiros estudos sobre medições de tráfego de rede foram realizados em redes locais, como as redes locais Ethernet. Essas redes são fáceis de se medir, por várias razões: i) uma rede local é tipicamente administrada com um bom nível de conhecimento da sua organização, o que torna o processo de análise de tráfego relativamente fácil. ii) em uma rede local Ethernet em broadcast os pacotes transmitidos são vistos por todos os computadores. Portanto, as medições de rede podem ser realizadas simplesmente configurando uma interface de rede em modo promíscuo, o que faz com que a interface receba e armazene os pacotes destinados a outros nós da rede.

Medição em Wide Area Network – WAN

Mais tarde, o trabalho de medição estendeu-se na recolha e análise de tráfego para ambiente WAN. Os grandes desafios foram o controlo administrativo da rede e questões sobre segurança e privacidade. Para organizações com um único ponto de acesso à Internet, dispositivos de medições podem ser colocados junto ao router de acesso da organização à Internet.

A medição em redes de computadores pode basear-se em medição de pacotes ou fluxos. [12]:

Medição Baseada em Pacotes

A medição baseada em pacotes consiste na captura e análise do cabeçalho dos mesmos. Exemplos de informações importantes obtidas no cabeçalho do pacote são o endereço IP de origem, o endereço IP de destino, a porta de origem, a porta de destino e o número do protocolo [12]. Actualmente, a colecta e análise estende-se muitas vezes ao payload (Deep Packet Inspection).

Medição Baseada em Fluxo

As ferramentas baseadas em fluxos permitem reduzir o volume do tráfego analisado da rede através da agregação de pacotes em fluxos de informação. Para isso, são utilizados cinco campos do cabeçalho dos pacotes no processo de formação de um fluxo que são: o endereço IP de origem, o endereço IP de destino, a porta de origem, a porta de destino e o protocolo da camada de transporte [12]. O Netflow da Cisco é um exemplo de ferramenta baseada em fluxos.

h. Alguns exemplos de ferramentas de gestão

Para medir o desempenho de uma rede é preciso seleccionar as métricas, métodos e ferramentas adequadas. Assim, depois de seleccionar as métricas que serão analisadas e os métodos a usar, o passo seguinte será seleccionar as ferramentas de colecta de dados e análise desses dados. Os dados obtidos são posteriormente apresentados de acordo com as métricas em gráficos ou tabelas. Segue-se uma breve descrição de algumas das ferramentas de medição e monitorização estudadas no âmbito deste modulo:

Cacti

Cacti é uma ferramenta que recolhe dados em rede de computador e exibe informações sobre o estado da rede, através de gráficos [13]. Foi desenvolvido para ser flexível de modo que seja adaptada facilmente às diversas necessidades, bem como ser fácil de usar. Com essa ferramenta é possível monitorar o estado de elementos de rede, aplicações, largura de banda utilizada e uso de CPU. O cacti é um front-end do RRDTool, que armazena todas as informações necessárias para criar gráficos e preenchê-los com dados em uma base de dados. A interface é completamente em PHP. Permite adicionalmente de manter gráficos e dados, utiliza também o protocolo SNMP para consulta de informações em elementos de redes e/ou programas que suportam tal protocolo. A sua arquitectura prevê a possibilidade de expansão através de plugins, que adicionam novas funcionalidades.

Nagios

É um software aberto (open-source) [14] que monitoriza serviços. O Nagios usa comandos e protocolos para teste do estado de diversos serviços tais como HTTP, FTP, SSH, PING, POP3 ou SMPT, sem necessitar de SNMP. A informação acedida torna possível obter uma visão geral dos serviços disponíveis da rede, assim como o seu desempenho, sem necessitar de configurar e instalar novo software nos agentes. A configuração dessa ferramenta consiste em configuração manual dos equipamentos e serviços a monitorizar.

Ntop

É uma ferramenta de monitorização e gestão de rede para sistemas UNIX/Linux e Win32 [15]. Esta ferramenta tem as seguintes características e funcionalidades: análise dos pacotes que passam na rede, listar e ordenar o tráfego de rede, de acordo com vários protocolos, exibir estatísticas de tráfego, armazenar estatísticas de forma permanentemente em base de dados, identificar passivamente várias informações sobre os hosts da rede, incluindo o sistema operativo e endereço de e-mail do utilizador da estação, exibir a distribuição do tráfego do protocolo IP entre vários protocolos da camada de aplicação, descodificar vários protocolos da camada de aplicação e inclusive os encontrados em softwares do tipo PPP e actuar como colector de fluxos gerados por routers e switches através da tecnologia NETFLOW. Essa ferramenta tem interface gráfica para gestão e visualização das informações para melhor entender o estado da rede.

Dude

O uso de ferramentas de medição adequadas em software ou hardware permitem recolha de informações detalhadas sobre a transmissão de pacotes na rede. Dude é um potente sistema de gestão de Redes, Dispositivos e Serviços [16] [17], mantido pela Mikrotik. Essa ferramenta poder ser utilizada como ferramenta de monitorização e como ferramenta de gestão de rede.

Resumo da Unidade

Nesta unidade, foram abordados aspectos relacionados com a gestão de redes de computadores, monitorização, modelo FCAPS, arquitectura de gestão e avaliação de desempenho. Em particular, foram apresentados os principais conceitos relacionados com o SNMP, as métricas de desempenho a utilizar, descreveu-se como efectuar uma abordagem sistemática à avaliação do desempenho das redes de computadores e algumas ferramentas de gestão.

Avaliação da Unidade

Verifique a sua compreensão!

Exercícios

Instruções

Estes exercícios permitiram verificar o estado dos conhecimentos dos alunos em relação da unidade de modelo de referencia.

Critérios de Avaliação

A avaliação deverá processar-se de uma forma contínua, sistemática e periódica. O tipo de avaliação corresponderá aos objectivos definidos na unidade.

Avaliação

1. As arquitecturas e modelos de gestão classificam as funções de gestão em cinco categorias, designadas áreas funcionais de gestão. Estas áreas funcionais não são estanques, portanto, existem interacções entre áreas funcionais de gestão. Qual é a relação existente entre gestão de configuração, gestão de desempenho e gestão de falha?
2. Qual é a função do Gerente e Agente na arquitectura de gestão de redes INMF
3. Explique objectivamente por que temos Management Information bases - MIB's.

4. Quais foram as necessidades da normalização das actividades de gestão de redes?
5. Enumere as três Arquitecturas mais Importantes da gestão de redes.
6. No SNMP é possível um Gerente enviar ou solicitar informação para outro Gerente?
7. O que acontece com Remote Monitoring MIB's (RMON) quando não há comunicação entre agente e gerente, justifique a sua resposta.
8. Os objectos de uma MIB são especificados usando a Abstract Syntax Notation One (ASN.1). Cada tipo de objecto é definido por três blocos lógicos, descreva a funcionalidade de cada um.

Leituras e outros Recursos

As leituras e outros recursos desta unidade encontram-se na lista de Leituras e Outros Recursos do curso.

Unidade 4. [Segurança de Hardware e Software]

Introdução à Unidade

A segurança da rede é o processo através do qual uma rede é protegida contra ameaças internas e externas de várias formas. A fim de desenvolver uma compreensão completa do que é segurança na rede, você deve entender as ameaças contra as quais a segurança da rede visa proteger. É igualmente importante para desenvolver um entendimento de alto nível dos principais mecanismos que podem ser postos em prática para impedir esses ataques.

A maioria das empresas hoje em dia fornecem serviços aos seus utilizadores através da rede. Portanto, o número de recursos (hardware e Software) que necessitam de ser protegidos aumentou de forma significativa. Nesta unidade apresentamos a lista dos recursos de rede que precisam ser protegidos contra diversos tipos de ataques.

Objetivos da Unidade

Após a conclusão do estudo desta unidade, deverá ser capaz de:

- Identificar o que pretendemos proteger.
- Determinar o que pretendemos proteger e contra o que pretendemos proteger
- Determinar a probabilidade de ameaças dos recursos
- Implementar medidas que protejam seus activos
- Rever o processo de forma contínua, e fazer melhorias cada vez que achar necessário

Termos-chave

Plano de segurança: Um plano de segurança é um documento que descreve como uma organização irá tratar as suas necessidades em relação à segurança.

A análise de risco: análise de risco é a avaliação dos riscos associados a um determinado evento ou acção. A análise de risco leva à compreensão da perda associada com o evento ou acção, a probabilidade de ocorrência de tais riscos e o grau em que podemos mudar o resultado.

A política de segurança: Uma Política de Segurança tem por objectivo possibilitar a gestão de segurança em uma organização, estabelecendo regras e padrões para protecção dos activos ou recursos.

Segurança física: Isso faz parte de segurança em causa com as medidas destinadas a proteger contra ameaças físicas externas, ameaças físicas internas e ameaças físicas humanas.

vulnerabilidade de segurança: é um ponto no qual o sistema é alvos suscetível a um ataque.

Ameaça à segurança: As ameaças são os principais e prováveis perigosa que uma empresa está sujeita.

Actividades de Aprendizagem

Actividade 4.1 - Plano de segurança

a. Introdução

Realizar encontros com utilizadores com base nas informações coletadas nas fases anteriores. Definir políticas de segurança que sejam adequadas a empresa em questão e que possam ser humanamente cumpridas sem afectar as actividades da empresa. Publicar as normas de segurança na intranet da empresa, certificar-se de que todos entendem e estão de acordo com as normas. As empresas necessitam de plano de segurança pois todos os dias novos utilizadores estão tentando descobrir a vulnerabilidade das redes de dados, seja de forma intencional ou por acidente, pois cada dia estamos mais dependentes dos sistemas de comunicação.

b. Politicas

Uma Política de Segurança tem por objectivo possibilitar a gestão de segurança em uma organização, estabelecendo regras e padrões para protecção dos activos ou recursos. E xistem alguns questões, tais como: Como lidar com riscos? Como lidar com utilizadores descontentes? E como lidar com usuários que provocaram um acidente que resultou em uma falha de segurança ou exposição? Primeiro, recomendamos que dentro da estrutura da organização tenhamos pelo menos uma pessoa responsável pelas políticas de segurança. O administrador de rede nem sempre poderá dar conta de todo o recado. Por isso, um profissional dedicado deve ser o responsável pela segurança da rede.

O perfil deste profissional deverá ser o de um gerente, de um diplomata, pois ele deverá criar regras que os outros funcionários deverão seguir, deverá indicar pessoas que investiguem um determinado acidente de segurança, deverá combater hackers, falar com fabricantes, lidar com a gerência, etc. Um funcionário que tenha fortes conhecimentos de tecnologias de rede e habilidade para lidar com pessoas.

Um outro funcionário que dentro das organizações sempre foi usuário dos sistemas computacionais é o advogado. Os advogados devem entender que tipos de ameaças

cibernéticas podem aparecer frente a uma empresa e trabalhar em conjunto com o Security Officer para punir culpados.

Geralmente, os advogados irão necessitar de um treinamento, assim como o pessoal de informática. Ao perceber que foram atacados, é comum aos administradores de rede sentirem raiva e terem vontade de responder. Neste caso, a vítima também pode se transformar em transgressor, o departamento jurídico deve ser acionado e informado. O departamento jurídico deve ter pelo menos um funcionário que entende "alguma coisa de redes e segurança da informação".

O documento que define a política de segurança da empresa deverá ser estruturado da seguinte forma:

Deve ter objectivo: Proteger os sistemas de informação da empresa, bancos de dados, sites, manter a credibilidade de confiança depositada pelos clientes, estabelecer critérios de uso correto dos sistemas de informação, medidas punitivas, garantir a continuidade de negócios mesmo sob ataque, minimizar os efeitos de ataques severos, proteger o activo e passivo da organização e informações de clientes e projectos considerados estratégicos e secretos.

Alvo, área de actuação: Sua empresa está fazendo uma política de segurança, para quê? O que ela quer proteger? Por exemplo, as regras de segurança são aplicadas ao banco de dados e ao site corporativo, ao parque de máquinas (impressoras e computadores), a informações sigilosas de clientes, projectos e protótipos, e-mails, etc. Fica a seu critério escrever, aqui, o que quer proteger.

Sobre o uso correto dos sistemas: Esta parte deverá conter os seguintes itens:

Sobre a internet: como os utilizadores devem usar a Internet, que sites devem ou não visitar.

Sobre o uso da intranet: Que partes do sistema que está na intranet é público? Que partes somente um determinado grupo de utilizadores pode acessar?

Sobre o uso do hardware: Os utilizadores podem vir trabalhar com notebooks próprios? ou notebooks da empresa? Como podemos garantir que seus notebooks não serão roubados e os dados também? Os funcionários podem levar disquetes para trabalhar em casa? Os funcionários podem trazer HD, Palms, CDs e Disquetes seus para dentro da empresa? Os funcionários tem permissão para concertar o próprio hardware?

Sobre o uso dos sistemas internos da empresa: Quem usa que sistema?

Sobre o uso do e-mail coorporativo: Todos têm acesso ao e-mail? É um Exchenge ou x.400?

Sobre o uso do acesso remoto: existe acesso remoto à intranet? Por quem? A que horas? De qual cidade? Ou de que Pais.

Sobre o uso de outros tipos de recursos que queira proteger.

Classificação do uso da informação: Crie uma tabela e classifique seus dados de acordo com os seguintes critérios: a) valor da informação para sua empresa e b) tipo de proteção necessária. A informação poderá classificada da seguinte forma:

TopSecret: Planos de expansão, investimentos, parcerias secretas, ou qualquer informação que sua empresa considerar tão segura que, se for exposta a espiões, concorrentes ou pública seria a morte imediata da empresa.

Secreta: Emails, qualquer informação que possa colocar a credibilidade e reputação da organização em desvantagem competitiva frente a seus concorrentes.

Interna: e-mails, comunicação interna da empresa, relatórios entre gerentes, etc.

Sectorial: Emails, comunicação interna sectorial, é o tipo de tráfego de dados que não deve percorrer por outros sectores, como, por exemplo, informações exclusiva da gerência ou informações exclusivas do sector de pessoal (por exemplo: folha de pagamento de salário)

Pública: De livre acesso a todos, inclusive aos que estão fora da empresa.

Sobre o tipo de proteção necessária:

Muito alta: Proteção muito forte, diversas soluções de hardware e software, inclusive segurança física.

Alta: Proteção forte, um mix de soluções de software e talvez, pelo menos, uma solução hardware.

Média: De dois a três mecanismos de proteção.

Pouca: Um mecanismo de proteção.

Nenhuma: Nenhum mecanismo de proteção.

Classificação de propriedade dos sistemas de informação:

Autor da informação: Possui os direitos sobre a propriedade intelectual.

Usuário: Pessoa que pode não ser o criador da informação, mas tem autorização para usá-la.

Tipos de usuário: Depende do tipo de sigilo que a informação terá: se o usuário pode apenas ler; se pode ler e alterar, executar, distribuir, etc.

Classificação dos tipos de riscos:

Crimes cibernéticos: O atacante passou bom tempo tentando derrubar sua empresa ou roubar dados que ele poderá se aproveitar depois.

Infractor cibernético: Ele achou uma falha no seu site, não estava procurando nada de específico e decidiu aproveitar-se da falha.

Acidentes: Devido a desconhecimentos operacionais, os próprios funcionários podem cometer erros ao usar os sistemas da empresa e isto poderá provocar uma falha de segurança.

Falhas de sistema: Por falhas no sistema, temos desde falhas de projeto que não previam a segurança até panes que podem comprometer a segurança.

Controle de acesso: Como sua empresa já classificou toda a informação e recursos que ela deseja proteger e já sabe quem são utilizadores, podemos criar uma tabela Informação x Utilizadores, na qual estabelecemos quem pode acessar o que.

Mecanismo de protecção: Para cada tipo de informação ou facilidade computacional, deverá ser criada uma tabela com os mecanismos de hardware e software necessários para sua devida protecção.

Treinamento de utilizadores: Estipular treinamento para os utilizadores para informá-los sobre a informação da protecção da informação e sua importância para o devido funcionamento da organização. Os utilizadores devem obrigatoriamente participar de um treinamento e palestras sobre conscientização sobre segurança. Os usuários devem ser conquistados, pois se sentirem-se oprimidos, podem se tornar futuros inimigos internos. Alerta sobre responsabilidades e punições. Cada reunião com os utilizadores deverá ser registrada.

Documento aos empregados: Deverá levar em consideração os seguintes itens:

Por que a informação é importante.

Uma descrição das informações sob responsabilidade desse funcionário.

Deixar claro que determinadas informações são confidenciais e importantes para a continuidade dos negócios.

Deixar claro quais informações o funcionário não poderá tornar públicas e quais são as barreiras de tráfego dessas informações dentro da organização (por exemplo: informações sobre salário devem circular apenas dentro do setor de recursos humanos).

Deixar claro sobre a responsabilidade do funcionário ao sair da empresa no final de expediente e sobre seu desligamento da empresa.

Procedimentos disciplinares, regras do jogo!

Observação: Algumas empresas podem exigir que o funcionário assine uma renúncia de propriedade intelectual, isto às vezes é feito por empresas de tecnologia de ponta, tudo o que o funcionário criar durante sua estadia como funcionário da empresa é de propriedade da empresa!!

1. Planeamento de auditorias:

   - Determinar um plano de acção.
   - Escolher os sistemas a serem testados.
   - Criar um cronograma.
   - Executar as auditorias.
   - Avaliar resultados.

2. Planeamento Pós-ataque

   - Toda e qualquer actividade suspeita já deverá ter sido percebida pelos sistemas de detecção de intrusão;
   - A atividades suspeitas devem ser relatadas ao gerentes de TI;

1. Verificar o nível de severidade do ataque e relacionar as medidas possíveis que poderão ser tomadas;

   - Isolar a área atacada;
   - Acionar os servidores de backup;
   - Acionar o departamento jurídico da empresa para avaliar a situação e decidir se as autoridades competentes devem ser alertadas;
   - Se necessário, alertar o provedor;
   - Verificar sistemas de logs;
   - Verificar se sistemas de acesso e senha foram ou não comprometidos;
   - Tentar identificar e esboçar a anatomia do ataque e perfil do atacante;
   - Tentar rastrear junto ao provedor de acesso os caminhos tomados pelo atacante;
   - Registrar todas as medidas tomadas para resolver o problema.

3. Criar a documentação final

   - 3.1 O organograma da organização;
   - 3.2 Diagrama da rede atualizado; P
   - 3.3 Planejamento estratégico da organização;
   - 3.4 Estrategias de TI;
   - 3.5 Descrição detalhada de processos organizacionais; 3.6 Os resultados das auditorias de segurança;
   - 3.6 Os planos de contingências da organização para a área de TI;
   - 3.7 Planos de instalações elétricas e telefônicas,
   - 3.8 Localização de extintores de incêndio;
   - 3.9 Políticas de acesso, senhas e backups;

- 3.10 Procedimientos administrativos dos administradores de rede;
- 3.11 Procedimentos para tratamentos de senhas;
- 3.12 Procedimentos para administração dos recursos ativos de rede;
- 3.13 Procedimentos para administração de logs;
- 3.14 Diagramas de aplicativos em desenvolvimento;
- 3.15 .Estruturas de dados;
- 3.16 Preparar uma análise de riscos para os componentes de informação relacionados no item 4, 5 e 6.

c. Requisitos de segurança

Os itens apresentados neste subunidade podem ser vistos como dicas (para alguns) ou requisitos. O conteúdo desta subunidade vai ajudar na hora de implementar a segurança na organização. Alguns itens, são auto-explicáveis e não possuem longos comentários.

Segurança Física

Manter um diagrama mostrando áreas de risco de segurança para os funcionários, colocar este diagrama em uma parede onde todos possam ver (num corredor, por exemplo), indicar no diagrama, saídas de incêndio, escadas de emergências, área de risco, extintores de incêndios, etc. Na maioria das empresas, isto não é de responsabilidade do administrador de redes ou do responsável pela segurança de informações (Security Officer), isto é de responsabilidade da Comissão Interna de Prevenção de Acidentes.

Segurança Lógica

Descrevemos abaixo várias dicas de segurança para estudar e implementar na sua rede. Algumas são tão óbvias, que são independentes de plataforma:

1. Desabilitar os Logins remotos aos finais de semana, por exemplo, as portas ftp e telnet.
2. Desabilitar os Logins remotos durante a noite, por exemplo, as portas ftp e telnet 22.
3. Fazer um levantamento de quem realmente necessita realizar um login remoto e habilitar o serviço que este usuário necessite somente naquela ocasião.
4. Instalar senhas no setup em todas as máquinas. Em algumas máquinas para evitar que o usuário entre no setup, em outras máquinas uma senha no boot.
5. Estabelecer um final de semana por mês para realização de atualização de vacinas em todas as máquinas, bem como reparos, diagnósticos e auditorias, o intervalo desta atualização deverá ser ditado pelas normas da empresa (ou diretivas de segurança).
6. Criar um grupo responsável por testar novos software, propor aquisição, e treinamento para os técnicos regulares, este grupo também poderia estar responsável por estudar assuntos relacionados com segurança.

7. O grupo de certificação de software também poderá realizar a certificação de hardware, liberando ou rejeitando hardware por considerá-lo inseguro, ineficiente, lento, de difícil manutenção ou outros critérios que a equipe queira adotar.

8. Procurar uma autoridade certificadora, e adquirir um certificado de site seguro para o servidor web. As autoridades certificadores além de realizar a emissão de certificados podem fornecer treinamento (www.safeweb.com.br).

9. Solicitar a emissão de um Certificado Digital para cada funcionário dentro da empresa perante uma autoridade certificadora.

10. Usar o protocolo DHCP, na rede interna da empresa, tentar evitar o uso do protocolo BOOTP; fornecendo IP dinâmicos para as máquinas clientes você diminui a possibilidade de ataque nas máquinas dos usuários.

11. Criar um mapa actualizado da rede da empresa, ilustrado áreas segundo grau de risco quanto a ataques de hackers, estas áreas poderão ter vários níveis de risco, nestes níveis são definidas políticas de operação.

12. Criar um servidor de backup (para o servidor web, dns, email, contas de usuários, arquivos de protocolo e arquivos para ftp, etc).

13. Manter um servidor de reserva fora da rede, que entraria em funcionamento quando um servidor de arquivos ou um servidor de produção estivesse comprometido. É similar ao caso anterior porém aplicado a servidores de arquivo e impressão.

14. Cria um plano de backup. Incluir o que deverá estar no backup, quem deverá realizar esta operação, periodicidade, mídias, etc.

15. Manter um mapa da rede atualizado, indicar uma pessoa para realizar esta tarefa mesmo que seja realizada com um ferramenta, mas alguém deverá pelo menos rever se o mapa da rede condiz com o mundo real.

16. Utilizar ferramentas para realizar a engenharia reversa da rede (network discovery), existem várias ferramentas que podem realizar esta função (Network Discovery da 3COM, NetView, NetCracker Designet, etc).

17. Indicar pelo menos um técnico e um formulário para que sejam coletadas informações dos usuários sobre as condições de operação da rede e determinados equipamentos. Críticas e reclamações sobre a rede devem ser escutadas. Principalmente aqueles que alegam que a rede está lenta em determinados períodos do dia.

18. Apagar contas de utilizador ou desabilitar as contas conforme o caso. O utilizador sai de férias, então sua conta é desabilitada até seu retorno.

19. Estabelecer como parte do procedimento de demissão, que os técnicos do laboratório recebem, do sector de pessoal, os nomes dos funcionários desligados para que suas contas na rede sejam desativadas.

20. Instalar o squid com regras para filtragem de conteúdo.

21. Criar grupos menos genéricos para acesso à rede, isto permite um melhor controle de acesso aos servidores, por exemplo ao invés de termos um utilizador chamado Guest ou Convidado, poderíamos ter grupos com os nomes de sectores com as contas de funcionários.

22. Separar a rede administrativa de outros tipos de redes interna (rede de testes, criar uma sub-rede para cada departamento, etc).

23. O uso de switches para a separação de redes em favor de hubs tende a evitar a espionagem de barramentos com sniffers.

24. Manter uma página do servidor web em um servidor interno, ou melhor, montar uma intranet isolada da rede externa, na qual os funcionários tenham apenas acesso pela rede interna da empresa.

25. Criar datas para testes de segurança, auditoria de segurança na rede, preferencialmente em finais de semana para não comprometer os sistemas de produção.

26. Criar regras de segurança para uso de máquinas, tipo: a) os funcionários não podem instalar programas nas máquinas, usar cd-rom, etc. Diversas políticas podem ser aplicadas e devem ser apoiadas pela direcção.

Resumo da Unidade

Esta unidade, fundamentos de segurança em redes, abordou os conceitos dos principais serviços de segurança integridade, autenticidade e autorização, e ainda analise de risco, politica de segurança e requisitos de segurança.

Avaliação da Unidade

Verifique a sua compreensão!

Exercícios

Instruções

Estes exercícios permitiram verificar o estado dos conhecimentos dos alunos em relação da unidade de modelo de referencia.

Critérios de Avaliação

A avaliação deverá processar-se de uma forma contínua, sistemática e periódica. O tipo de avaliação corresponderá aos objectivos definidos na unidade.

Avaliação

1. Em um ambiente coorporativo, com muitas informações sigilosas, podem ser utilizadas as políticas de segurança, ou seja, conjuntos de regras, leis e práticas de gestão que visam a protecção dos seus dados e sistemas. Para isso, primeiro, uma política de segurança deve envolver as decisões sobre o que é importante ou não dentro daquela empresa, o que envolvevários profissionais da empresa. Mas, não é só nas empresas que as políticas de segurança podem ser aplicadas. Elas também devem ser aplicadas na sua rede local. Existem vários tipos de mecanismos que implementam as políticas de segurança e que chamamos de mecanismos de segurança.
2. Estabeleça as diferenças entre políticas de segurança e mecanismos de segurança.
3. Indique os principais mecanismos de segurança.
4. Qual a diferença entre firewall e IDS?
5. Em sua opinião por que são usados sistemas biométricos para fazer autenticação de utilizadores?
6. Explique qual a diferença entre autenticação e autorização.
7. Indique dois modelos de controlo de acesso.

Leituras e outros Recursos

As leituras e outros recursos desta unidade encontram-se na lista de Leituras e Outros Recursos do curso.

Unidade 5. Manutenção e Resolução de Problemas

Introdução à Unidade

Vamos concluir este módulo de administração de redes com um tópico que todos nós achamos que nunca precisaremos de nos preocupar, mas todos precisam saber. É quase impossível uma rede funcionar sem acontecer algo de errado. Isto é, não existem duas redes iguais mesmo com mesma topologia. A resolução de problemas de uma rede local pode ser um trabalho sério e difícil de realizar. Muitos factores entram em jogo. Um problema que parece fácil de resolver pode tornar algo totalmente difícil de resolver. Algumas vezes a resolução do problema pode levar uma hora mas outras vezes a resolução do mesmo problema pode levar um dia inteiro. É por isso que esta unidade é um guia que pode usar para ajudá-lo (a) a ter uma ideia de como esta actividade de administração é complexa. Esperamos que o que aqui vai aprender lhe dê a mão quando for resolver um problemas nas tuas actividades futuras.

Objetivos da Unidade

Após a conclusão desta unidade, deverá ser capaz de:

- Compreender a importância da manutenção e resolução de problemas como actividade essencial de Administração da Rede.
- Conhecer e diferenciar os procedimentos de resolução de problemas na rede.
- Compreender a necessidade de elaboração do plano de manutenção e os seus procedimento de acordo com as normas de gestão de redes.
- Conhecer a importância do backup dos servidores e equipamentos da rede.
- Aplicar as medidas e procedimentos adequados para resolução de problemas da rede.

Termos-chave

Manutenção: Trata-se da medida preventiva e correctiva tomada para garantir uma infra-estrutura de rede confiável.

Resolução de problemas: Solução de problemas de rede são as medidas colectivas e processos utilizados para identificar, diagnosticar e resolver problemas nas redes de computadores.

Gestão de falhas: é processo de detectar, registar e alertar os administradores do sistema de problemas que possam afectar as operações do mesmo.

desastre: Este é um evento, como um acidente ou de uma catástrofe natural, que causa danos a um componente ou componentes.

Backup: Este é o processo de fazer cópias de segurança de dados de um lugar para outros lugares com objectivo de recuperar posteriormente.

Recuperação: Esta é a área de planeamento de segurança que lida com a proteção de configuração de rede de uma organização para recuperar os dados armazenados no lugar.

Actividades de Aprendizagem

Actividade 5.1 - Resolução de problemas

5.1.1 Introdução

Não é uma coisa boa quando um evento catastrófico prejudica a funcionalidade da rede. Muitas vezes podemos ter sorte de ter um problema que já tenha acontecido antes e resolver em pouco tempo mas outras vezes, pode haver uma necessidade de pegar um telefone e fazer uma chamada para um amigo da área para ajudar a resolver o problema da sua rede local.

Como discutimos nas unidades anteriores, a estação de gestão (NMS) de rede é uma opção ideal para alerta de qualquer evento que pode acontecer na rede. Quando ocorre um problema que pode afectar o fluxo normal dos dados, a estação de gestão de rede dá um alerta. O alerta pode ser visual ou áudio (beep).

5.1.1 O que de errado pode acontecer ?

Você sabe com certeza que tomou todas as precauções na concepção da sua rede. Ela deve ser confiável e rápida ... muito rápida. Por uma questão de conhecer a importância dos serviços fornecidos pela sua rede, você fez questão de colocar em uma estação de gestão na rede. Então, o que pode dar errado? A resposta a essa pergunta é, quase nada. E é isso que é tão desafiador para o profissional administrador de rede. A seguir está uma lista de possíveis problemas que pode encontrar ao solucionar um problema em sua rede:

- Cabo de dado danificado
- uma fibra-ptica com problema
- atenuação do sinal
- insuficiência de largura de banda

Até agora analisamos exemplos de algumas situações que pode se deparar ao monitorar e gerir a sua rede. Antes de aprofundar, sem ficar apenas na tarefa de resolução de problemas,

vamos dar uma olhada em algumas das perguntas instantâneas que podem vir à mente quando acontece um problema na rede. Se é notificado (a) de que algo está errado na rede, deve fazer as seguintes perguntas:

- Quantos utilizadores estão afectados?
- É apenas um utilizador que está enfrentando o problema ou vários?
- É o problema previsto? Se assim for, tem um plano de acção?
- já viu o problema antes?
- Qual é o impacto na rede? Em outras palavras, que nós são afetados?
- Quantos domínios são afetados?

Entender o problema é fundamental para solucioná-lo de forma eficaz. Sem uma boa compreensão do problema, pode proceder por caminhos errados para resolução do problema.

5.1.2 A abordagem pro-activa contra re-activa

É incrível como muitos administradores de rede continuam a trabalhar no modelo re-activo na gestão das suas redes. Não estamos aqui para julgar ninguém, mas realmente não faz sentido, na parte da gestão das redes, continuar com um modelo re-activo em vez do modelo pro-activo. Muitos autores defendem que a solução de problemas de rede de forma pro-ativa é uma das coisas mais importantes que pode fazer para diminuir o tempo que leva para chegar a uma resolução, quando ocorrer um problema na rede local.

5.1.3 A base de gestão

Para saber que algo está errado, tem que saber o que é certo (neste cenário, no que diz respeito à sua rede). Em outras palavras, o que é normal? A linha mestre de gestão da rede é definida pelo comportamento normal da rede.
Por exemplo, o comportamentos de protocolo e comportamento de tráfego na redes são apenas um par de itens que podem ser usados como uma comparação quando algo simplesmente não parece certo. Aqui estão algumas dicas que pode usar para observação da sua rede:

- Análise de tráfego
- Estatísticas apresentados pela estação de gestão em gráfico
- Determinação dos paramentos acertáveis para melhor funcionamento da rede

É muito importante ter uma base para comparação, quando o utilizador final diz que a rede está mais lenta do que o normal. Assim será capaz de comparar os dados em tempo real para ver se, de facto, a questão de lentidão reside na rede ou não. É uma excelente maneira de reduzir o tempo que leva para achar o culpado quando há um problema na rede. Manter um registro de captura de informação de gestão é uma prática muito importante e tem que ser um hábito normal. Vai descobrir que isso é útil não só para chegar a uma solução, mas também em provar que algo está errado. Muitas vezes, precisa ter a prova para mostrar quando pedimos uma ajuda.

5.2.4 Documentação Pro-activa

Ter documentação que descreve a topologia física e lógica é muito essencial para a resolução de problemas da rede de forma pro-activa. Ainda mais fundamental é ter certeza de que esta documentação é actual e actualizada em todos os momentos. Por exemplo, não faz absolutamente nada de bom manter diagramas de rede que não acompanha as mudanças que estão sempre a acontecer na rede. Por documentação, não significa que deve manter uma cópia em papel de tudo o que tem; em vez disso, estamos sugerindo o armazenamento de informações críticas em qualquer meio eletrónico (cópia eletrônica) eletrônico ou em formulário (papel).

Ao fazer isso estará oferecendo uma visão geral de alguma documentação recomendada para manter e ter prontamente disponíveis. Como muitas coisas na rede, pode olhar para esta informação como um modelo de referência. Se achar que quer manter alguma dessas informação sinta-se livre para adicionar a esta lista qualquer coisa que sinta que você precisa adicionar.

Certifique-se que sempre a documentação importante da rede existe e é regularmente actualizado. Crie o hábito de mudar a documentação básica como as mudanças introduzidas na rede. Além da documentação básica, manter bons registros que pertencem às topologias físicas e lógicas da rede é também um bom hábito. Tenha em mente que até mesmo o sistema de monitoramento de rede mais impressionante não vai fazer qualquer trabalho bonito se não conseguir localizar um nó com problema. No mínimo, é importante manter um registro dos seguintes procedimentos:

- Um diagrama de topologia lógica
- Um diagrama de topologia física
- Uma planilha ou outra listagem de onde os nós de usuário residem
- Documentação que diz respeito à DMZ
- Documentação que contém informações relativas a nós fora da DMZ

Documentação que descreve a localização e nó de interligação para:

- Network firewalls
- Network management stations
- Mainframe servers
- Remote access servers
- Routers
- Switches Layer 4-7 nodes
- Wiring closets
- VLANs
- VPNs

- Informações relativas à LAN para conectividade WAN
- Informações relativas a conectividade campus-to-campus

- Lista de documentação:
– Network layer addressing
– Major node names
– LAN identification
- Node serial number
- Node maker and model names/number
- Software and hardware version numbers
- Licensing information
- Circuit identification for WAN
- Connections Geographical information for nodes listed above, including address and contact name and number
- Node access login information
- Backup copies of:
– Node configurations
– System logs
– System software
- Name and number for support with the ISP
- Name and number for support for the vendors of nodes and application in use within the LAN

5.2.5 Outras medidas pró-activas

Estabelecer uma linha de base para a sua rede não é a única coisa que pode fazer para simplificar a tarefa de resolução de problemas, não eixtem medidas em demasiado. Pode tomar algumas outras medidas pro-activas para ajudar a manter a rede em execução e obtê-la de volta para execução quando tem um problema:

- partilha de conhecimento
- ferramentas adequadas
- requisitos de conhecimento
- peças de reposição

A sua rede será tão eficaz se seguir todas essas recomendações pró-activas que poderá ajudar a aliviar um pouco a dificuldade na solução de problemas.

5.2.6 Ferramentas de solução de problemas

Quando existe um problema na rede, é importante ter acesso a algumas ferramentas importantes que podem auxiliar a resolução de problemas. A maioria dos nós da rede tem logs de eventos que auxiliam no diagnóstico de problemas com um nó específico. Além disso, você pode consultar as tabelas de endereços MAC na Camada 2 nós, tabelas de roteamento IP na Camada 3 nós, caches ARP, estatísticas de linha de comando, etc., porque há muitos tipos diferentes de nós, e os comandos para reunir esses dados são específicos, é quase impossível introduzir muitos deles neste livro. Felizmente, existem algumas ferramentas e utilitários que estão disponíveis para você usar, seja embutido, download ou outro disponível

para compra:

Helpful TCP/IP Utilities

Ping

Traceroute

Netstat

Route

Arp

Ipconfig

Resumo da Unidade

Nesta unidade, foram abordados aspectos relacionados com manutenção e resolução de problemas em redes de computadores. Em particular, foram apresentados os principais conceitos relacionados resolução de problemas e procedimentos a seguir, ainda nesta unidade foram apresentadas as ferramentas e documentos necessários que facilita o processo de resolução de problemas.

Avaliação da Unidade

Verifique a sua compreensão!

Exercícios

Instruções

Estes exercícios permitiram verificar o estado dos conhecimentos dos alunos em relação da unidade de modelo de referencia.

Critérios de Avaliação

A avaliação deverá processar-se de uma forma contínua, sistemática e periódica. O tipo de avaliação corresponderá aos objectivos definidos na unidade.

Avaliação

Utilizando as informações do header dos protocolos Ethernet, IP, ICMP, TCP e UDP, e também outras informações como número total de pacotes enviados/ recebidos, contadores de tempo, etc, responda às questões a seguir:

1. Que informações devem ser monitoradas para identificar a origem e o destino dos pacotes?

2. Quais as informações que devem ser monitoradas e calculadas para identificar o volume de pacotes que trafegam na rede, dos seguintes protocolos:

- IP
- ICMP
- TCP
- UDP
- http (WEB)
- SMTP (e-mail)
- SSH

3. Quais as informações que devem ser monitoradas e calculadas para identificar a frequência de envio de mensagens ICMP ECHO REQUEST?

4. Quais as informações que devem ser monitoradas e calculadas para identificar a frequência de pedidos de conexão TCP para a mesma aplicação de uma máquina servidor?

5. Que informações devem ser monitoradas para identificar a ocorrência de umaenchente de pacotes ICMP Echo Request para um endereço de broadcast para uma rede específica?

6. Quais as informações que devem ser monitoradas e calculadas para identificar:

O número total de pacotes enviados e recebidos por uma máquina (host).

O volume de tráfego em bits por segundo (bps) que trafegam na rede.

O volume de tráfego de entrada e saída (enviados e recebidos) em bps que no enlace de dados (canal de comunicação) entre um provedor Internet e seu cliente.

7. Quais os aspectos que devem ser monitoradas para criar uma matriz de tráfego que contenha a origem e o destino do tráfego, e a identificação do protocolo de aplicação ou de controle utilizado entre origem e destino. É importante observar que a mesma origem e o mesmo destino podem ter comunicações simultâneas para serviços diferentes.

Leituras e outros Recursos

As leituras e outros recursos desta unidade encontram-se na lista de Leituras e Outros Recursos do curso.

Laboratório: Instalação e Configuração do DNS

1.1 Objectivos

Instalação e configuração do DNS

criar dominio di.up.ac.mz

1.2 Servidor DNS Local

O Domain Name System é um protocolo fundamental no funcionamento da internet, tal como a conhecemos na actualidade. Trata-se de um serviço imprescindivel para correcto funcionamento de qualquer rede informática, mesmo que essa rede não disponha de ligação à internet. O DNS consegue disponibilizar informação sobre nomes e endereços de máquinas e serviços.

1.2.1 Objectivo

Install Bind9

local DNS Cache

1.2.2 Resources required

Personal Computer with 2GB of RAM

Internet access for install

Virtualization Software (Virtualbox or VMware)

Operation System (Debian 7.0)

Internet

1.2.3 Time required

1 hr for Installation Dind9

2 hr for configuration

1.2.4 Descrição do Laboratório

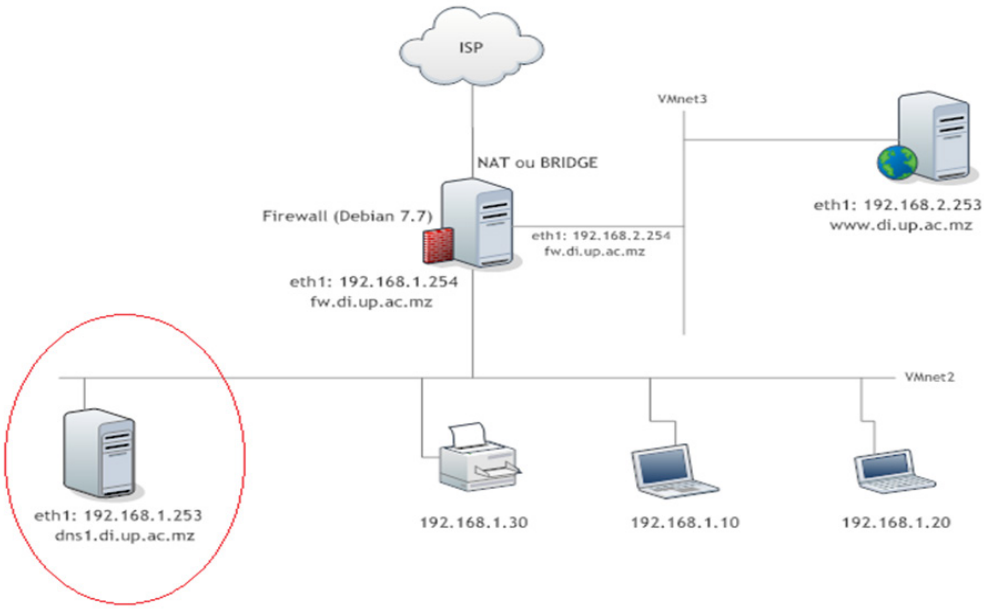
Embora se possa atribuir nomes aos diversos sistemas de uma rede, estes não se conseguem reconhecer entre eles sem um sistema de resolução de nomes. Para que um sistema consiga localizar o endereço IP associado ao nome de outro sistema, é necessário que este esteja registado num servidor DNS, de modo a permitir a resolução de nomes.

A resolução de nomes converte nomes de sistemas no seu endereço IP e vice-versa. Assim, a configuração consiste, basicamente na criação de 2 zonas, uma zona (zone "di.up.ac.mz") que converte nomes em endereços IP e outras zonas (zone "1.168.192.in-addr.arpa" e "2.168.192.in-addr.arpa") que converte endereços IP no respetivo nome de sistema.

Servidores de nomes e zonas

Os programas que armazenam informações sobre o espaço de nomes de domínio são chamados de servidores de nomes. Os servidores de nomes geralmente possuem informações completas sobre uma parte do espaço de nomes de domínio (uma zona), que eles carregam de um ficheiro ou de outro servidor de nomes. O servidor de nomes passa então a ter autoridade sobre aquela zona.

Topologia (Topology)



Instalação (Installation)

```
root@dns1:~# apt-get␣update
```

```
root@dns1:~# apt-get ␣install ␣ bind9
```

Configuração do ficheiro named.conf.local

```
root@dns1:# cd /etc/bind/  <enter>
```

```
root@dns1:/etc/bind# nano named.conf.local  <enter>
```

named.conf.local

```
zone "di.up.ac.mz" {
        type master;
        file "/etc/bind/db.di.up.ac.mz";
};
zone "1.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.1.168.192";
};
zone "2.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.2.168.192";
};
```

Configuração do ficheiro db.di.up.ac.mz

```
root@dns1:# cd /etc/bind/  <enter>

root@dns1:/etc/bind# cp db.local db.di.up.ac.mz  <enter>

root@dns1:/etc/bind# nano db.di.up.ac.mz  <enter>
```

db.di.up.ac.mz

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     dns1.di.up.ac.mz. admin.di.up.ac.mz. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
        NS      dns1.di.up.ac.mz.
        MX      10 mail.di.up.ac.mz.
dns1    IN      A       192.168.1.253
mail    IN      A       192.168.1.252

di.up.ac.mz.    IN      A       192.168.1.253
Web             IN      A       192.168.2.253

fw              IN      A       192.168.1.254
fw              IN      A       192.168.2.254

www             IN      CNAME   web
```

Configuração do ficheiro db.1.168.19

```
root@dns1:# cd /etc/bind/  <enter>

root@dns1:/etc/bind# cp db.127  db.1.168.192  <enter>

root@dns1:/etc/bind# nano db.1.168.192  <enter>
```

db.1.168.192

```
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     dns1.di.up.ac.mz. admin.di.up.ac.mz. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
                        NS      dns1.di.up.ac.mz.

253     PTR     dns1.di.up.ac.mz.
254     PTR     fw.di.up.ac.mz
100     PTR     xp.di.up.ac.mz
```

Configuração de resolve no Linux

A configuração de resolver em Linux, ou seja, a configuração do sistema enquanto cliente do serviço DNS, utiliza alguns ficheiros de configuração que administrador deve conhecer. Os ficheiros de configuração relevante neste âmbito são:

Ficheiro de configuracao	Propósito de utilização
/etc/host.conf	Definição da ordem das consultas ao ficheiro hosts e serviço DNS
/etc/hosts	Definição local de correspondências entre endereços e nomes de servidores
/etc/resolv.conf	Definição do domínio DNS e dos endereços dos servidores locais de DNS

Configuração do ficheiro host.conf

```
root@dns1:# cd /etc/  <enter>

root@dns1:/etc# nano host.conf  <enter>
```

```
  GNU nano 2.2.6           File: /etc/host.conf

# The "order" line is only used by old versions of the C library.
order hosts,bind
multi on
```

Configuração do ficheiro resolv.conf

```
root@dns1:# cd /etc/  <enter>

root@dns1:/etc# nano resolv.conf  <enter>
```

Configuração do ficheiro hosts

```
root@dns1:# cd /etc/  <enter>

root@dns1:/etc# nano hosts  <enter>
```

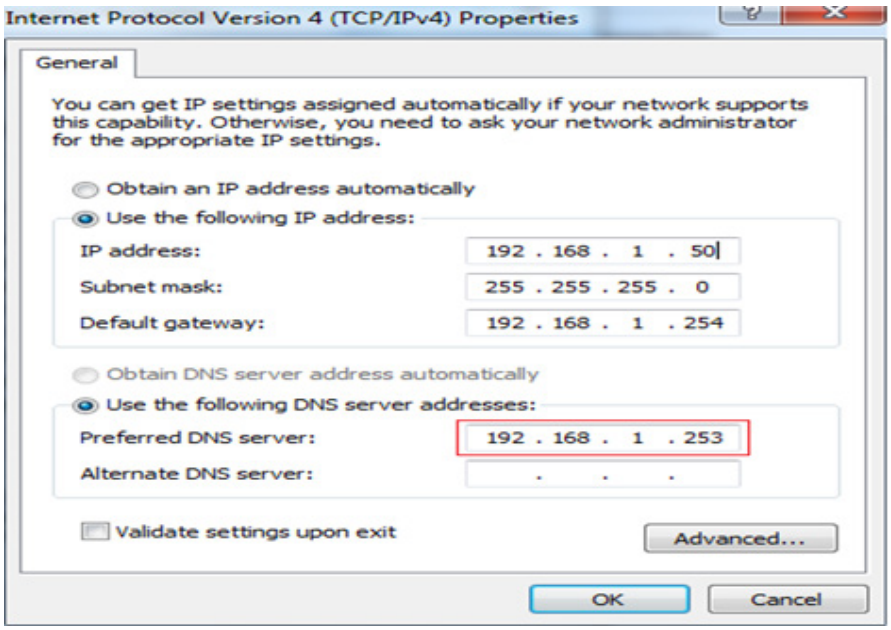
Configuração de cliente no Linux

No caso de sistemas Linux, editar o ficheiro /etc/resolv.conf e acrescentar ou substituir o nameserver com o endereço IP do nosso servidor:

```
root@dns1:~# nano /etc/resolv.conf

# [...]

nameserver 192.168.1.253

# [...]
```

Configuração de cliente no Windows

Para Sistemas Operativos Windows é indicar, nas propriedades do protocolo Internet (TCP/IPv4)) da ligação de rede, o endereço do nosso servidor DNS (192.168.1.253) como sendo o servidor DNS preferido.

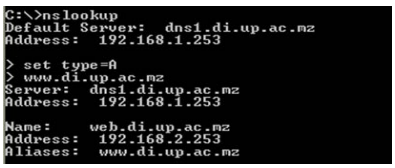


1.2.5 *Resolução de nomes*

Assim, quando nos referimos ao sistema "dns1", este será procurado no domínio "di.up.ac.mz.", resultando no nome "dns1.di.up.ac.mz".

No Windows

Obter um endereço IP, dado um nome



Obter o nome, dado endereço

No Linux

Obter um endereço IP, dado um nome

```
root@dns1:~# nslookup dns1
Server:        127.0.0.1
Address:       127.0.0.1#53
dns1.di.up.ac.mz       canonical name = dns1.di.up.ac.mz
Name:   dns1.di.up.ac.mz
Address: 192.168.1.253
```

```
root@dns1:~# nslookup 192.168.1.253
Server:        127.0.0.1
Address:       127.0.0.1#53

 253.1.168.192.in-addr.arpa      name = dns1.di.up.ac.mz
```

1.2.6 Critérios de Avaliação

Avaliação (Meta e Prazos)

Meta	Resultado esperado
Meta 1: ● Planeamento e especificação do projecto ● Planeamento do projecto · Definir o método de trabalho	Relatório e apresentação/ discussão
Meta 2: ● Firewall ● Instalação e configuração do firewall	Relatório e apresentação/ discussão
Meta 3: ● Serviço de DNS ● Instalação e configuração do Cache DNS ● Instalação e configuração do DNS local	Relatório e apresentação/ discussão
Meta 4: ● Teste de serviços .	Relatório (10%) e apresentação/ discussão (90%)

References

[1] KUROSE, James, ROSS Keith, "Computer Networking – A Top-Down Approach" 6ed, 2012

[2] DROMS, Ralph, LEMON Ted, "The DHCP HANDBOOK", 2ed,2002

[3] JANG, Michael, "Ubuntu Server Administration", 2009

[4] Uyless Black, "IP Routing Protocols", Publisher: Prentice Hall

[5] Ravi Malhotra, "IP Routing", Publisher: O'Reill

Referências do Curso

[1] José Maurício Pinheiro, Infra-Estrutura Eléctrica para Rede de Computadores,1st ed., Ciência Moderna, Ed., 2008.

[2] Raj Jain, The Art of Computer Systems Performance Analysis: Techniques for

experimental design, measurement, simulation and modeling, Wiley And Sons, Ed.York New, 1991.

[3] James D. Mccabe, Network Analysis, Architecture, and Design, 3rd ed. Burlington:Morgan Kaufmann, 2007.

[4] William Stallings, SNMP, SNMPv2, SNMPv3 and RMON1 and 2, 3rd ed., Addison Wesley Longman, Ed., 1999.

[5] Douglas R. Mauro, Kevin J. Schmidt, Help for system and network administrators:

Essential SNMP, 1st ed. America: O'Reilly & Associates, 2001.

[6] Véstias Mário, Redes CISCO para profissionais, 4th ed., FCA, Ed. Lisboa,Portugal, 2009.

[7] Willig Andreas, "Performance Evaluation Techniques," Summer 2004, April 2005.

[8] Richard Blum, Network Performance Open Source Toolkit: Using Netperf,

tcptrace, NIST Net, and SSFNet, Carol Long, Ed. Indianapolis, United States:

Wiley Publishing, 2003.

[9] Raj Jain, Hassan Mahbub, High performance tcp/ip networking concepts, issues and solutions, Prentice Hall, Ed., 2003.

[10] George Coulouris, Jean Dollimore, Tim Kindberg, Distributed Systems: Concepts and Design, 4th ed., Pearson Education Limeted, Ed. London, 2005.

[11] Carey Williamson, "Internet Traffic Measurement," IEEE Internet Computing, vol. 5, no. 6, p. 9, November 2001.

[12] Solange Lima, Network traffic measurement, 2009/2010, Textos de apoio ao

Mestrado.

[13] Cacti. (2010, January) Cacti. [Online]. http://docs.cacti.net/

[14] Nagios. (2010, January) The Industry Standard in IT Infrastructure Monitoring.

[Online]. http://www.nagios.com/products/nagiosxi/

[15] Ntop. (2010, March) Ntop. [Online]. http://www.ntop.org/documentation.html

[16] Mikrotik. (2010, January) DUDE. [Online]. http://www.mikrotik.com/thedude.php.

[17] Coppini Andrea. (2010, january) Buiding Custom Probes and Configuring devices via SNMP. [Online]. http://mum.mikrotik.com/presentations/CZ09/Building custom-probes-and-SNMP.pdf

[18] Edmundo Monteiro, Fernando Boavida, Engenharia de redes de informáticas, 8th ed., FCA, Ed. Lisboa, Portugal, 2000.

[19] José Gouveia, Alberto Magalhães, Redes de Computadores, 8th ed., FCA, Ed. Lisboa, Portugal, 2009.

Exame final da Unidade

Sede da Universidade Virtual africana

The African Virtual University
Headquarters

Cape Office Park

Ring Road Kilimani

PO Box 25405-00603

Nairobi, Kenya

Tel: +254 20 25283333

contact@avu.org

oer@avu.org

Escritório Regional da Universidade Virtual Africana em Dakar

Université Virtuelle Africaine

Bureau Régional de l'Afrique de l'Ouest

Sicap Liberté VI Extension

Villa No.8 VDN

B.P. 50609 Dakar, Sénégal

Tel: +221 338670324

bureauregional@avu.org