**Camadas Modelo OSI**

* **Física:**A camada física trata da **transmissão de bits brutos** por um canal de comunicação e cabeamento.
* **Enlace:**A principal tarefa da camada de enlace de dados é **transformar um canal de comunicação bruto em uma linha que pareça livre de erros de transmissão** não detectados para a camada de rede (ela permite a **identificação física** dos dispositivos de rede.)
* **Rede:**A camada de rede é responsável pelo **endereçamento dos pacotes de rede, também conhecidos por datagramas**, associando endereços lógicos (IP), de forma que os pacotes de rede consigam chegar corretamente ao destino.
* **Transporte:**A função básica da camada de transporte é **receber os dados da camada acima dela, dividi-los em unidades menores caso necessário (segmentos), repassar essas unidades à camada de rede e assegurar que todos os fragmentos chegarão corretamente à outra extremidade**. É **executado apenas nos sistemas finais** (Realiza **controle de fluxo**, **ordenação de pacotes** e **correção de erros**, sendo considerada a primeira **camada fim-a-fim.)**
* **Sessão:**A camada de sessão permite que os **usuários de diferentes máquinas estabeleçam sessões entre eles**, provê a **delimitação e sincronização da troca de dados**, incluindo os meios de construir um **esquema de pontos de verificação e de recuperação**.
* **Apresentação:**A camada de apresentação, ao invés de preocupar-se com a movimentação de bits, **preocupa-se com a sintaxe e a semântica das informações transmitidas (TCC – Tradução, Compreensão, Criptografia)**
* **Aplicação:**A camada de aplicação corresponde às aplicações (programas) no topo da camada OSI que serão utilizados para **promover uma interação entre a máquina destinatária e o usuário da aplicação**. (É responsável pelos **PROTOCOLOS**)

**ESTABELECER**a comunicação --> **SESSÃO**

**MANTER**a comunicação --> **TRANSPORTE**

CNAME = Nome canônico  
  
O **CNAME**é um recurso que permite o servidor DNS (Servidor de Nome de Domínio)**atribuir diferentes nomes** (alias ou podemos chamar de rótulos)**para serviços diferentes que rodam em um mesmo servidor.**  
  
Para entender melhor, vamos a um exemplo:  
  
Digamos que no mesmo servidor há o serviço de hospedagem de sites, ou seja, webserver, e também o de disponibilização de arquivos por meio de FTP, rodando em portas diferentes.  
  
Para que o usuário tenha acesso a esses serviços de forma amigável, com o CNAME pode-se configurar um nome para o serviço de hospedagem, por exemplo, **www**.questoesdeconcursos.com.br e para o FTP um outro nome **ftp**.questoesdeconcurso.com.br.

***SNMP***

**ASN.1 (Abstract Syntax Notation One): É um padrão ISO que define, entre outras coisas, uma representação para os dados enviados por uma rede.**

**SMI (Structure of Management Information): é uma linguagem específica, usada para garanir que os objetos das MIBs sejam padronizados.**

**MIB (Management Information Base): Base de informações de gerenciamento, define as partes específicas da informações.**

**Primitivas SNMP**

GET - ler valor na MIB

GETNEXT - descobrir o próximo objeto

GETBULK - grande quantidade de informação do agente para o gerente

SET - escrever valor na MIB

TRAP - agente informa ao gerente a ocorrência de um evento

INFORM - comunicação gerente-gerente

REPORT - reporta problemas com o processamento de mensagens

O SNMP (*Simple Network Management Protocol*) permite o monitoramento e o controle de roteadores e outros dispositivos de rede. As informações de gerenciamento que um dispositivo precisa manter, as operações permitidas sobre tais informações e os seus significados são descritos na MIB (*Management Information Base*).

O padrão SMI (*Structure of Management Information*) especifica que a descrição dessas informações de gerenciamento deve ser feita com a ASN.1.

A extensialidade do SMI é feito geralmente com o uso de **sintaxe em ASN** (é uma notação que permite definir tipos de dados simples e complexos e especificar valores que estes tipos podem assumir), ou seja, ele utiliza os seus tipos básicos para melhor gerenciamento de objetos gerenciados.

A dúvida seria se poderia utizar por exemplo XML, o ASN é uma linguagem extremamente segura utilizada em comunicações entre bancos satélites:

"Contrary to XML (and JSON), ANS.1 is **not** a data interchange format, but primarily a language to define what the exchanged data means (plus a whole set of ways to encode that data). "

O SNMP versão 3 foi criado para suprir uma necessidade padronização que se fez necessária com as várias variações do SNMPv2 quem tentavam criar soluções de segurança para o protocolo. O SNMPv3 teve como base as definições das variações SNMPv2u e SNMPv2\*.

Além das definições das **questões de segurança**, o projeto do SNMPv3 também objetivou uma padronização de implementação das entidades (agente/gerente), modularizando suas funcionalidades, o que facilita a evolução de alguns mecanismos do protocolo sem exigir que novas versões sejam lançadas. Outros objetivos eram a manutenção de uma estrutura simples, facilitar a integração com outras versões e, sempre que possível, reaproveitar as especificações existentes.

O SNMPv3 incorporou o SMI e o MIB do SNMPv2, assim como também utilizou as mesmas operações do SNMPv2, apenas com uma reescrita da norma para uma compatibilização da nomenclatura.

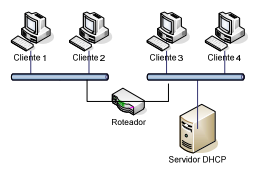
Parte superior do formulário

**UDP** - Entrega dos pacotes, não confiável, não agrupa os pacotes e não confirma a chegada. Não avisa sobre falhas; ex: ao fazer download de um arquivo, apos a finalização, ao abrir o arquivo, descobre que está corrompido.

**TCP** - Entrega dos pacotes, confiável, garante a chegada, agrupa os pacotes na ordem que chegam, controla o fluxo (confirma a chegada dos pacotes), se houver perda de pacotes, avisa o usuário sobre a falha!

**FTP** - Protocolo de transferência de arquivos, usado por e-mails, por ex, ao fazer download de arquivos.

**HTTP** - Protocolo de Hipertexto (montagem da web), é um protocolo de comunicação, não criptografado

**ICMP** - (Internet Control Message Protocol - Protocolo de Mensagens de Controle de Internet) é um protocolo que permite gerenciar as informações relativas aos erros nas máquinas conectadas. Devido aos poucos controles que o protocolo IP realiza, ele não corrige estes erros mas os mostra para os protocolos das camadas vizinhas. Assim, o protocolo ICMP é usado por todos os roteadores para assinalar um erro, chamado de Delivery Problem ou, em português, Problema de Entrega.

O roteador precisa ter agente DHCP ativado para permitir que os clientes 1 e 2 recebam a configuração IP do servidor DHCP.

"Para permitir o funcionamento do DHCP em redes segmentas, foi definido um mecanismo complementar denominado “***agente relay***” (RFC1542). O agente relay é um software que roda em um roteador ou computador (existe implementações do agente relay para sistemas operacionais, como o Linux). O agente relay é configurado para escutar mensagens BOOTP em broadcast e propagá-las em unicast para um roteador DHCP especifico".

Parâmetros que podem ser passados são:

-IP do cliente

-IP do gateway da rede

-IP do servidor DNS

-IP do servidor NTP

-IP do Broadcast da rede

O endereço MAC já "nasce" com a placa/interface de rede do host. Além disso é um identificador fixo(e não dinâmico) da placa de rede e a princípio "não muda".

Algumas mensagens da arquitetura Cliente-Servidor DHCP

* **DHCPDISCOVER**- Mensagem enviada pelo cliente em broadcast para localizar um servidor DHCP;
* **DHCPOFFER** - Mensagem enviada pelo servidor ao cliente em resposta à mensagem DHCPDISCOVER;
* **DHCPREQUEST** - Mensagem enviada pelo cliente ao servidor DHCP solicitando os parâmetros de configuração da rede (Endereço IP, Máscara, Gateway, etc);
* **DHCPACK** - Mensagem enviada pelo servidor ao cliente com os parâmetros de configuração, incluindo o comprometimento do endereço de rede;
* **DHCPRELEASE** - Mensagem enviada pelo cliente ao servidor para liberar o IP da máquina cliente.

**O protocolo TCP**é orientado à conexão, realiza controle de transmissão, é confiável, verifica erros, permite a recuperação de pacotes perdidos, elimina pacotes duplicados, recupera dados corrompidos, faz controle de fluxo e de congestionamento e ainda entrega os pacotes na sequência correta.

**O protocolo UDP**é simples, sem garantia de entrega, não-confiável, não orientado à conexão, os dados são transmitidos apenas uma vez, pacotes corrompidos são descartados, porém é de alta eficiência e velocidade em comparação com o TCP. Mais usado para transmissão de áudio e vídeo em tempo real.

**OSPF e BGP**são protocolos de roteamento.

**RSTP e MSTP** são variações do Spanning Tree Protocol (STP)

**EAPS** é um protocolo proprietário da Extreme Networks para controle de Loop em redes em Anel de alta disponibilidade.

**Estados possíveis de portas - STP  - Spanning Tree Protocol -  802.1d**

**Blocking,**

**Listem,**

**Learning,**

**Forwarding,**

**Disabled**

**RSTP - Rapid Spanning Tree Protocol - 802.1w**

**Discarding**

**Learning**

**Forwarding**

Durante uma transferência de arquivos utilizando o FTP o seguintes passos são tomados:

O cliente solicita a abertura de conexão ao servidor através da porta de controle. O servidor aceita a solicitação e mantém a conexão de controle aberta. É nessa conexão que o cliente deve informar qual arquivo deseja obter ou enviar. O servidor aceita a solicitação do cliente e envia os dados para o cliente abrindo uma nova conexão - a conexão de dados. Essa conexão existe até que o dado seja transferido por completo. Após a transferência o servidor fecha a conexão de dados até que o cliente solicite um novo arquivo.

Se o cliente não desejar mais enviar ou receber dados ao servidor então aquele deve encerrar a conexão. Caso contrário, o servidor poderá encerra-la devido ao time-out.

**Classe A**  
Primeiro octeto entre 1 e 126  
(Em binário, o primeiro bit do primeiro octeto é zero)  
Máscara padrão: 255.0.0.0

**Classe B**  
Primeiro octeto entre 128 e 191  
(Em binário, o primeiro bit do primeiro octeto deve ser 1 e o segundo bit 0)  
Máscara padrão: 255.255.0.0

**Classe C**  
Primeiro octeto entre 192 e 223  
(Em binário, os dois primeiros bits devem ser 1 e o terceiro 0)  
Máscara padrão: 255.255.255.0

RIP - Vetor de Distância

OSPF - Estado de enlace

BGP - Vetor de Caminho

**BGP** é o protocolo usado para troca de informações sobre roteamento da internet e ele é usado por ISP’s (Internet Service Providers). A versão usada atualmente é o BGP-4.Comumente, as empresas e universidades usam em suas redes, protocolos de roteamentos internos IGP. Vários clientes compartilham o mesmo AS de um ISP, dessa forma, na borda do AS do  ISP é usado o BGP para trocar informações de rotas com a internet para seus clientes.

O **OSPF** (Open Shortest Path First), traduzindo ficaria assim: "**Primeira Rota Aberta Mais Curta**" é um protocolo intradomínio baseado no roteamento com **estado de enlaces**. Na terminologia do OSPF, enlace é a denominação de uma conexão.

É bom lembrar que o OSPF, apresenta menor tempo de convergência que o RIP.

**Agumas características do protocolo RIP:**

**-- Protocolo de roteamento de vetor distância;**

**-- Como métrica, usa a contagem de saltos;**

**-- Mensagens enviadas por broadcast a cada 30 segundos;**

**-- Cada nó constrói uma sequência unidimensional contendo as distâncias para todos os outros nós;**

**-- As distâncias válidas são de 1 a 15 (saltos), com 16 representando infinito, limitando o para redes relativamente pequenas.**

**-- Trabalha na camada de aplicação;**

**RIP – porta 520**

**RIPng (para IPv6) – porta 521**

LDAP - Porta padrão: 389

HTTP - Porta padrão: 80

HTTPS - Porta padrão: 443

FTP - Portas padrões:  21 para conexão de controle - 20 para conexão de dados

O SNMP foi criado para facilitar o monitoramento e gerenciamento de redes permitindo que uma ferramenta de gerenciamento possa trabalhar com produtos e serviços de diversos fabricantes.

Em SNMP, o item a ser monitorado ou gerenciado é um agente. Quem consulta (GET) ou solicita modificações(SET) é um gerente. O agente tambem tem a função de gerar alertas (TRAP).

Sistemas de monitoramento de redes como HP Open View, IBM Tivoli, Nagios e Zabbix suportam SNMP nativamente para monitoramento e gerenciamento SNMP.

O sistema gerente pode usar estes alertas para gerar alarmes visuais ou usar ferramentas de comunicação como SMS e e-mail para avisar os responsáveis.

O agente SNMP, instalado no item a ser gerenciado, contempla uma tabela de informações que pode ser consultada ou modificada pelo sistema gerente. Desta forma, é possível por exemplo consultar como está o tráfego de rede em determinada porta de um switch ou qual o estado de memória em uma máquina Java.

**PAM**

O PAM (Pluggable Authentication Modules) é o serviço responsável por realizar a autenticação de usuários nos ambientes Linux/Unix. Através do PAM e de suas bibliotecas, é possível configurar um esquema de autenticação segura para qualquer aplicação de forma transparente.

O pacote libpam-ldap é o plugin do LDAP para o PAM, ou seja, ele é que permitirá ao PAM autenticar usuários armazenados no diretório LDAP. O PAM apenas realiza a autenticação dos usuários que foram reconhecidos durante a pesquisa do NSS, ou seja, é necessário instalar e configurar o módulo libnss-ldap antes do libpam-ldap para que a autenticação dos usuários do diretório LDAP seja efetuada.

**LDAP significa Lightweight Directory Access Protocol**

• protocolo leve para acessar serviços de diretório.

• roda em cima do protocolo TCP/IP .

\* arquitetura cliente/servidor

\* foi inicialmente usado como uma interface para o X.500

\* Organiza as entradas em árvores hierárquicas;

• camada de aplicaçãa

pelas entradas do serviço de diretório organizadas em uma estrutura de árvore hierárquica conhecida como DIT − Directory Information Tree.

O **LDAP** (Lightweight Directory Access Protocol - Protocolo de acesso aos diretórios leves) é um protocolo padrão que permite gerenciar diretórios, ou seja, acessar bancos de informações sobre os usuários de uma rede por meio de protocolos TCP/IP. Geralmente, os bancos de informações são relativos a usuários, mas eles também podem ser usados para outros fins, como gerenciar o material de uma empresa.

O LDAP fornece ao usuário métodos que lhe permitem se conectar, desligar, procurar e comparar informações e inserir, alterar e excluir entradas. Por outro lado,**o protocolo LDAP (na sua versão 3) propõe mecanismos de codificação (SSL, etc.) e autenticação (SASL) que permitem proteger o acesso às informações armazenadas no banco.**

**Portanto o LPAD suporta SIM mecanismos de segurança e acesso a cliente.**

***Tipos de Registros DNS***

o   **SOA (Start of Authority)** – Apresenta o início dos dados de um domínio; Também define o nome da zona e do servidor da zona;

o   **A (Address)** – Contém o endereço IPv4 de um registro;

o   **AAAA (Quad-A)** – Contém o endereço IPv6 de um registro;

o   **CNAME (Canonical Name)** – É o segundo nome ou apelido (alias) de um registro de domínio;

o   **PTR (Pointer)**– Tipo de registro utilizado para configuração de DNS reverso; é o inverso de A(ipv4) ou de AAAA(ipv6)

o   **NS (Name Server)** – Representa os nomes dos servidores DNS autoritativos presentes em um domínio;

o   **MX (Mail Exchange)** – Exibe o nome dos servidores de e-mail do domínio;

o   **MINFO (Mailbox Info)** – Contém o endereço de e-mail para contato dos responsáveis pelo domínio;

o   **HINFO (Host Info)** – Possui informações sobre o host que provê o serviço de DNS;

o   **TXT (Text)**– Contém alguma informação textuais sobre o domínio;

o   **SPF (Sender Policy Framework)** – tentativa de controle de falsos emails. Permite definir os endereços das máquinas autorizadas a enviar emails.

o   **SRV (Service)** – define a localização de serviços disponíveis em um domínio.

**POP3**

Porta padrão 110 - NÃO criptografada

Porta**995**– Porta SSL / TLS, também conhecida como POP3S.

**IMAP**

Porta padrão 143 - não criptografada

Porta **993** – Porta SSL / TLS, também conhecida como IMAPS

**SMTP**

Porta **465** – Porta SSL / TLS, também conhecida como SMTPS

***VoIP***

Serviços como VoIP (voz sobre IP) necessitam de um protocolo de tempo real, **como os protocolos RTP/RTCP.** Alguns protocolos: **SIP**, **SDP**, **RTP** **MGCP** e o **H.248**.

H.323 é uma recomendação criada pela ITU para o estabelecimento, controle e término das chamadas, ou seja, é uma recomendação que especifica os protocolos de sinalização e controle das ligações. Ela é mais antiga e complexa, atualmente está sendo menos usada nos sistemas VoIP.

**SIP**

O Session Initiation Protocol (SIP) foi padronizado pela IETF e é descrito na Request for Comments (RFC) 3261. O SIP é um módulo projetado para interoperar bem com aplicações da Internet já existentes para a utilização da tecnologia VoIP.

Com o SIP é possível efetuar chamadas entre computadores, entre telefones IP, e de um computador para um telefone comum, havendo o gateway apropriado entre a Internet e o sistema de telefonia tradicional neste último caso. O SIP somente configura, gerencia e encerra as chamadas, ele é um protocolo de sessão. Outros protocolos são encarregados pelo transporte de dados, normalmente o protocolo UDP, por motivos de desempenho. Assim o SIP fornece seus próprios mecanismos de confiabilidade, mas o TCP também pode ser usado. O protocolo RTP se encarrega pelo tráfego em tempo real da informação, muito importante na comunicação de voz, e consequentemente em conjunto com o RTP, também há o RTCP, que controla os fluxos de dados em tempo real.

A telefonia por internet utiliza o protocolo SIP na Camada de Aplicação e o protocolo UDP da Camada de Transporte. SIP usa UDP/TCP.

**RTP e RTCP**

O protocolo Realtime Transport Protocol (RTP) é responsável pelo fluxo de voz já convertida em dados na tecnologia VoIP. A voz precisa ser transmitida em tempo real e é o protocolo RTP que possibilita essa transmissão. Ele é utilizado tanto na pilha de protocolos H.323 como com o SIP. Já o protocolo Realtime Transport Control Protocol (RTCP) monitora a entrega dos dados, além de ter funções de controle e identificação.

**MGCP**

O Media Gateway Control Protocol (MGCP) foi definido na RFC 2705 da IETF e é usado para controlar as chamadas nos gateways do sistema VoIP. O MGCP implementa uma interface de controle usando um conjunto de transações do tipo comando/resposta que criam, controlam e auditam as chamadas. Estas mensagens usam como suporte os pacotes UDP da rede IP, e são trocadas para o estabelecimento, acompanhamento e finalização das ligações. O MGCP tem como finalidade principal a simplificação do uso da tecnologia VoIP, eliminando a necessidade de terminais complexos para a telefonia IP.

**MEGACO/H.248**

O MEdia GAteway COntrol (MEGACO) realiza as mesmas funções do MGCP, ele foi criado com o esforço conjunto da IETF e ITU. Ele pode ser utilizado em um gateway com funções implementadas em único equipamento ou em um gateway com funções que podem ser distribuídas por vários equipamentos.

O MEGACO também possui uma interface de sinalização para diversos sistemas de telefonia, tanto fixa como móvel. Esse protocolo representa uma alternativa ao MGCP, pois enfoca requisitos técnicos e recursos de conferência multimídia omitidos pelo seu antecessor.Ele também controla melhor a execução ordenada de comandos por meio de transações, e define modos de transporte específicos das mensagens sobre outros protocolos além do UDP, como o SCTP, um protocolo de transporte mais recente, por exemplo.

Com o funcionamento destes protocolos estabelecendo a comunicação entre os equipamentos, o próximo assunto a ser abordado são as aplicações da tecnologia VoIP, para que uma chamada telefônica seja efetuada entre uma origem e um destino numa rede IP.

Tendo em vista que são possíveis diversos algoritmos de compactação, é necessário um protocolo para permitir que os terminais negociem o algoritmo que vão usar. Esse protocolo é chamado H.245. Ele também negocia outros aspectos da conexão, como a taxa de bits.

"O **ICMP** permite que os roteadores relatem erros ou informações sobre circunstâncias inesperadas. Ele é usado por hospedeiros e roteadores para troca de informações da camada de rede entre si; a utilização mais comum é para comunicação de erros. O ICMP deve ser permitido em uma rede para que os hosts enviem mensagens de erro ou de controle para outros hosts da rede.

É frequentemente considerado parte do IP, mas, em termos de arquitetura, está logo acima do IP. As mensagens ICMP são carregadas dentro de datagramas IP como carga útil IP, exatamente como segmentos TCP ou UDP, que também são carregados como carga útil. No caso de erro num datagrama ICMP, nenhuma mensagem de erro é emitida para evitar um efeito “bola de neve” no caso de incidente sobre a rede."

**PPP (Point-to-Point Protocol)** é um protocolo para transmissão de pacotes através de linhas seriais. O protocolo PPP suporta linhas síncronas e assíncronas. Normalmente ele tem sido utilizado para a transmissão de pacotes IP na Internet.

O Point-to-Point Protocol é projetado para transportar pacotes através de uma conexão entre dois pontos. A conexão entre os pontos deve prover operação full-duplex sendo assumido que os pacotes são entregues em ordem. Estas características são desejadas para que o PPP proporcione uma solução comum para a conexão de uma grande variedade de Hosts, Bridges e Routers.

O PPP é composto basicamente de três partes, sendo que a interação entre elas obedece a um diagrama de fases:

Encapsulamento de datagramas

Link Control Protocol( LCP )

Network Control Protocols( NCPs )

Para ser suficientemente versátil e portável para uma grande variedade de ambientes, o PPP provê um Link Control Protocol.

O Link Control Protocol é usado para automaticamente concordar sobre as opções de formato de encapsulamento, lidar com variações nos limites de tamanho dos pacotes, detectar loops infinitos, detectar erros de configuração, iniciar e terminar a conexão.

Opcionalmente o LCP pode prover facilidades de autenticação de identificação e determinação de quando o link está funcionando apropriadamente ou quando está falhando.

**Algoritmos de criptografia do WPA-2**

O WPA2 ainda dá suporte ao algoritmo de criptografia do TKIP, mas também introduziu uma opção nova e mais segura que costuma ser chamada de Counter Mode with Cipher Block Chaining Message Authentication Code ProtocoL (CCMP) que por sua vez fornece o uso do AES como algoritmo de criptografia a ser utilizado.

O CCMP usa CBC-MAC para integridade da mensagem.

"***Controle de fluxo envolve impedir que os transmissores sobrecarreguem os receptores***. Controle de congestionamento envolve impedir que muitos dados sejam injetados na rede, fazendo com que switches ou enlaces fiquem sobrecarregados. Ou seja, controle de fluxo é um problema fim a fim, enquanto o controle de congestionamento se preocupa com o modo como hosts e redes interagem" **Redes de Computadores – Peterson.**

**Wireless**

**"Não há sobreposição entre quaisquer dois canais se, e somente se, eles estiverem separados por quatro ou mais canais. Em particular, o conjunto dos canais 1, 6 e 11 é o único conjunto de três canais não sobrepostos. Isso significa que um administrador poderia criar uma LAN sem fio  [...] instalando três APs [...] na mesma localização física, designando os canais 1, 6 e 11 aos APs e interconectando cada um desses APs com um comutador.". Para que não ocorra sobreposição de canais de radio­ frequência adjacentes, o número máximo de Access Points que podem ser instalados naquele local são três.**

1000 BASE-TX  Cabo UTP 6 ou +  (alcance 100m)

1000 BASE-T    Cabo UTP 5 ou +  (alcance 100m)

1000 BASE-SX  Fibra Multimodo  (alcance até 550m)

1000 BASE-LX  Fibra Monomodo  ou Multimodo (alcance máximo 3km)

**1000 BASE-CX  2 Pares de cabo STP (alcance máximo 25m)**

802.11a velocidades de 54 Mbps freq de 5,1 Ghz a 5,8Ghz 12 canais ñ sobrepostos

802.11b  velocidade de 11 Mbps frequência de 2.4 GHz 3 canais ñ sobrepostos

802.11g velocidade de 54 Mbps freq de 2,4 GHz WPA criptografia TKIP e AES  3  ñ sob

802.11n velocidade de 54 Mbps a 300 Mbps freqüência: 2,4 GHz e/ou 5 GHz MIMO OFDM

**IEEE 802.11ac (**2014) - Faixa de Frequência de 5.0 GHz - Velocidade acima de 1.5 GHz

Parte superior do formulário

Parte superior do formulário

**Jitter** é uma variação estatística do **atraso** na entrega de dados em uma rede, ou seja, pode ser definida como a medida de variação do atraso entre os pacotes sucessivos de dados. Observa-se ainda que uma variação de atraso elevada produz uma recepção não regular dos pacotes.

***Proxy***

O **proxy web**possui tanto função de servidor quanto de cliente. É servidor quando possui os objetos solicitados pelos navegadores e lhe envia as respostas. É cliente quando não possui algum objeto solicitado e precisa requisitá-lo ao servidor web. Os proxies vêm sendo muito usados nas empresas, com o intuito de acelerar o acesso à Internet e evitar investimentos em ampliação de largura de banda.   
  
O **proxy reverso** é um servidor instalado entre a internet e os servidores web internos de uma empresa. As requisições externas são direcionadas a um servidor interno por meio de um roteamento feito pelo proxy.

Um **proxy reverso** é um servidor de rede geralmente instalado para ficar na frente de um servidor Web. Todas as conexões originadas externamente são endereçadas para um dos servidores Web através de um roteamento feito pelo servidor proxy, que pode tratar ele mesmo a requisição ou encaminhar a requisição toda ou parcialmente a um servidor Web, que tratará dela.

Um proxy reverso repassa o tráfego de rede recebido para um conjunto de servidores, tornando-o a única interface para as requisições externas. Por exemplo, um proxy reverso pode ser usado para balancear a carga de um cluster de servidores Web. O que é exatamente o oposto de um proxy convencional, que age como um despachante para o tráfego de saída de uma rede, representando as requisições dos clientes internos para os servidores externos à rede a qual o servidor proxy atende.

***Principais características***

**Segurança**: o servidor proxy pode oferecer uma camada adicional de defesa através da separação ou isolamento do servidor que está por trás de um proxy reverso. Essa configuração pode inclusive proteger os demais servidores da rede, principalmente pela obscuridade.

**Criptografia**: a criptografia SSL pode ser delegada ao próprio servidor proxy, em vez dos servidores Web. Nesse caso, o servidor proxy pode ser dotado de aceleradores criptográficos de alta performance.

**Balanceamento de carga:** o proxy reverso pode distribuir a carga para vários servidores, cada servidor responsável por sua própria aplicação. Dependendo da arquitetura da rede onde o servidor proxy reverso está instalado, o proxy reverso pode ter que modificar as URLs válidas externamente, para os endereços da rede interna.

**Cache**: um proxy reverso pode aliviar a carga dos servidores Web através de um cache para o conteúdo estático, como, por exemplo, imagens, e também conteúdo dinâmico, como, por exemplo, uma pagina HTML gerada por um Sistema de Gerenciamento de Conteúdo. Um cache desse tipo pode satisfazer uma quantidade considerável de requisições, reduzindo de forma significativa o servidor Web. Outro termo utilizado é Acelerador Web. Essa técnica é utilizada nos servidores da Wikipédia.

**Compressão:** um servidor proxy pode otimizar e comprimir o conteúdo, tornando o acesso mais rápido.

**Colher de chá:** uma página dinamicamente gerada pode ser produzida e enviada instantaneamente para o servidor proxy, que pode enviá-la aos poucos para o cliente requisitante. A aplicação Web não precisa ficar esperando (e consumindo recursos do servidor) porque o cliente apresenta restrições de capacidade para receber conteúdo solicitado.

Em uma rede local do tipo Ethernet, um *firewall* que atua na camada de enlace pode ser configurado para permitir ou negar o tráfego de dados por endereço MAC. (Questão correta).

**Comentario**: para quem teve a mesma dúvida que eu, cabe destacar que o Firewall pode, sim, atuar na camada de enlace. Acreditava que era somente na de rede.

**Filtragem de pacotes** é o bloqueio ou liberação da passagem de pacotes de dados de maneira seletiva, conforme eles atravessam a interface de rede. Em sistemas Linux, por exemplo, a filtragem de pacotes é implementada diretamente no kernel.**Esses filtros inspecionam os pacotes com base nos cabeçalhos de transporte, rede ou até mesmo enlace**. Os critérios mais utilizados são os endereços IP e portas TCP/UDP de origem e destino.

(...)

Apesar de se tratar de um conceito geralmente relacionado a proteção contra invasões**, o firewall não possui capacidade de analisar toda a extensão do protocolo, ficando geralmente restrito ao nível 4, de Transporte, da Camada OSI.**

**WEP** → RC4 (cifra de fluxo simétrica)

**WPA** → RC4 + TKIP

**WPA2** → AES (cifra de bloco simétrica) + TKIP

***O protocolo 802.1x*** possui características que são complementares a redes sem fios , pois permite***autenticação*** baseada em métodos já consolidados, como o**RADIUS (Remote Authentication Dial-in User Service)**, de forma escalável e expansível. Desta maneira é possível promover um único padrão de *autenticação*, independentemente da tecnologia (vários padrões de redes sem fio, usuários de redes cabeadas e discadas etc.) e manter a base de usuários em um repositórios únicos, que seja em banco  de dados convencional, LDAP ou qualquer outro reconhecido pelo servidor de autenticação.

O **proxy** **transparente** é uma arquitetura que permite que o navegador cliente não saiba da existência do proxy. Ele acha que está solicitando o recurso diretamente ao servidor original; o proxy encarrega-se de capturar e processar a solicitação. Sua principal característica é não precisar sair configurando nos navegadores.

***Redes WI-FI***

(1997) 802.11    -> 2.4GHz --> até 2 Mbps --> DSSS.  
(1999) 802.11a  -> 5.0GHz --> até 54 Mbps --> OFDM.  
(1999) 802.11b  -> 2.4GHz --> até 11 Mbps --> OFDM.  
(2003) 802.11g  -> 2.4GHz --> até 54 Mbps --> DSSS, OFDM.  
(2009) 802.11n  -> 2.4 e 5.0 GHz --> até 300Mbps, e até 600 Mbps teoricamente --> OFDM.  
(2012) 802.11ad -> 60 GHz --> até 6.75 Mbps --> OFDM.  
(2013) 802.11ac -> 5.0 GHz --> até 433 Mbps, e mais de 6Gbps teoricamente --> SC, OFDM.

*"Um* ***Bastion Host*** *é o termo aplicado a um host que age como um check-point entre a sua rede e a Internet, ou entre subredes da Intranet. Ele pode ser associado de várias maneiras à entrada de um edifício - todos devem passar por aquele ponto tanto para entrar quanto para sair do edifício. Para um Bastion Host que está conectado à Internet, maior atenção deve ser dada à segurança - é o ponto mais exposto e, por essa razão, deve ser o mais forte.*

*O Bastion Host seria o ponto de entrada, tipicamente dos seguintes serviços:*

*Sessões de E-mail que estejam chegando (SMTP) e distribuí-las para o site;  
Requisões de FTP para o servidor de FTP anônimo;  
Para consultas ao servidor de DNS interno.  
Serviços para redes externas, podem ser tratadas de uma das maneiras seguintes:*

*Configuração de Packet Filtering nos roteadores externo e interno para permitir que clientes externos acessem servidores externos diretamente;  
Configurar servidores proxy para rodarem no Bastion Host (se o firewall da rede estiver configurado para tal) para permitir que clientes internos acessem servidores externos indiretamente. O Packet Filtering pode ser configurado para permitir também que clientes internos comuniquem com os servidores proxy no Bastion Host e vice-versa, mas para proibir que haja comunicação direta entre os clientes internos e o mundo exterior."*

**Internet, somente pacotes com IP, destinados ao bastion host, possuem permissão de entrada.**

Um  Bast host  protege as redes internas atuando como uma **camada de defesa** entre a **Internet e uma intranet**. Um bast host  é um computador totalmente exposto ao ataque. O sistema está no lado público da zona desmilitarizada (DMZ), desprotegido por um firewall ou roteador de filtragem. Frequentemente, os papéis desses sistemas são fundamentais para o sistema de segurança da rede.  Em suma, um Bast host é um servidor endurecido que se espera que seja atacado. Não confia em nada e ninguém.

Bast Host é uma  uma estrutura para fortificação para proteger as coisas por trás.

Aba 13 – firewall wireless