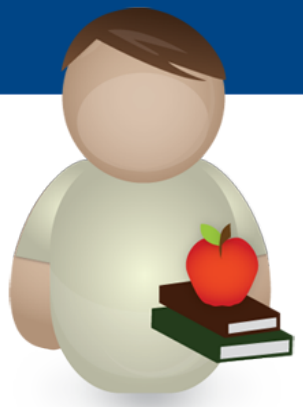


Disciplina:
Segurança de Redes

Professor:
Roitier Campos

Conceitos Gerais sobre Administração de Redes

Funções da Administração de redes

Planejar

Implementar

Monitorar

Proteger

Dimensionar

Auditar

Dia a dia do Administrador

- Instalações físicas e lógicas;
- Implementar, monitorar e auditar a rede;
- Atualização de serviços e correção de falhas de segurança;
- Análise de incidentes;
- Inovação tecnológica – Para o usuário e para a gerencia da rede;
- Documentação;

Recomendações

Visitas regulares a Fóruns, Listas de Discussões, sites de hackers, etc.

Arquitetura TCP/IP

Sistema utilizado para garantir a interoperabilidade entre variados tipos de dispositivos como:

Celulares;

Computadores;

Tablets;

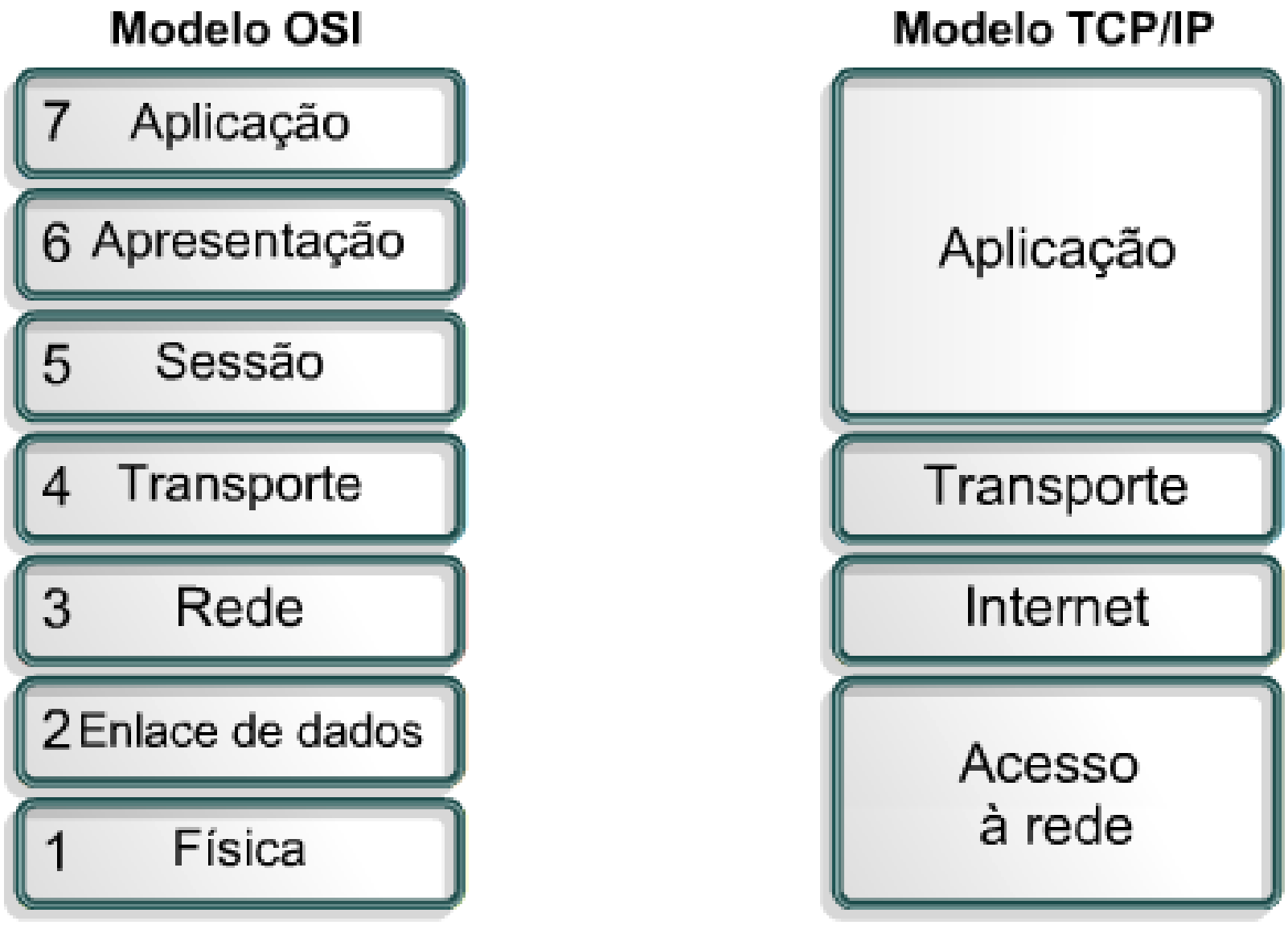
Notebooks.

Modelos de Referência

Ajudam na compreensão do funcionamento da rede, sendo que para isso utiliza-se da classificação dos protocolos quanto às suas atribuições, distribuindo-os em camadas.

- RM-OSI
- TCP/IP

RM-OSI X TCP/IP



RM-OSI X TCP/IP

O RM-OSI, apesar de ser considerado ideal, teve sua adoção global dificultada por vários fatores, dentre os quais podemos relevar a diversidade de protocolos.

Já o TCP/IP tornou-se o padrão em função da minimização do conjunto de protocolos e da sua ampla e gratuita disseminação no Unix.

Sugestão de Literatura:

Livro: Redes de Computadores 4 – Andrew S. Tanembaum

Capitulo 1.4.1 - O modelo de referência OSI;

Capitulo 1.4.2 - O modelo de referência TCP/IP;

Capitulo 1.4.3 - Uma comparação entre os mo delos de referência OSI e TCP/IP

Modelo de referência híbrido

5	Camada de aplicação
4	Camada de transporte
3	Camada de rede
2	Camada de enlace de dados
1	Camada física

Nivel de enlace - Ethernet

O Padrão Ethernet, (Padrão IEEE 802.3) apesar de fazer parte da camada de enlace, camada 2 (OSI) é comumente conhecido como endereço físico ou endereço MAC (Medium Access Control):

- Padrão IEEE 802.3
- Endereços de 48 bits (ff:ff:ff:ff:ff:ff);
- Controle de acesso ao meio (CSMA/CD).

Tipos de endereços físicos

Endereços fisicos assumem três tipos:

- Unicast – (identifica uma interface);
- Multicast – (indentifica um grupo);
- Broadcast - (identifica todos os computadores da rede),

Formato do quadro Ethernet

Uma interface de rede “só recebe“ quadros Ethernet endereçados ao seu próprio endereço físico ou para o endereço brodcast.

No entanto, podemos configurar uma placa para a aceitação indiscriminada de quadros Ethernet. (Modo promisc)

Preâmbulo (8 bytes)	Endereço de destino (6 bytes)	Endereço de Origem (6 bytes)	Tipo (2 bytes)	Dados (46–1500 bytes)	FCS (4 bytes)

Address Resolution Protocol (ARP)

Sempre que duas ou mais máquinas precisam se comunicar, elas precisam saber o endereço físico do receptor.

O Protocolo ARP (Nível 2) é responsável por fazer essa identificação. Para isso, cada nó (equipamento nível 2 ou superior) da rede tem uma tabela ARP informando IP e MAC de cada host conectado a ele.

A atualização dessa tabela é feita através do TTL, Time to Live, que é um tempo pré estabelecido para que a tabela renove os dados, afim de garantir que nenhum equipamento ficará relacionado a um IP indiscriminadamente.

Protocolo IP

Protocolo responsável pela identificação lógica de hosts em uma rede. Atualmente se o protocolo assume duas formas, como segue:

- IPv4 – 32 bits
- Ipv6 – 128 bits

É o ICANN (Internet Corporation for Assigned Names and Numbers, substituindo o IANA, Internet Assigned Numbers Agency, desde 1998) que está encarregado de atribuir endereços IP públicos, isto é, os endereços IP dos computadores directamente ligados à rede pública de Internet.

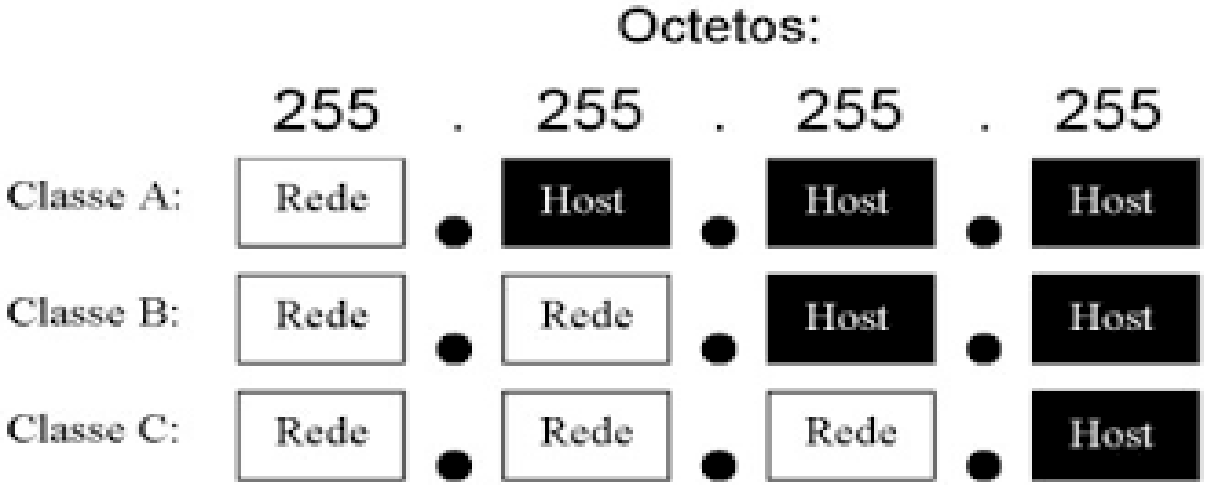
Obs: Utilizaremos o Ipv4 como referência para nossos estudos.

Endereço IP

Endereço de rede composto por 32 bits divididos em 4 octetos (quadros de 8 bits);

192.168.0.1 – 11000000.10101000.00000000.00000001

Todas as máquinas de uma rede compartilham de um mesmo prefixo em seu endereço. Esse prefixo identifica a rede a qual esse endereço pertence.



Netid e Hostid

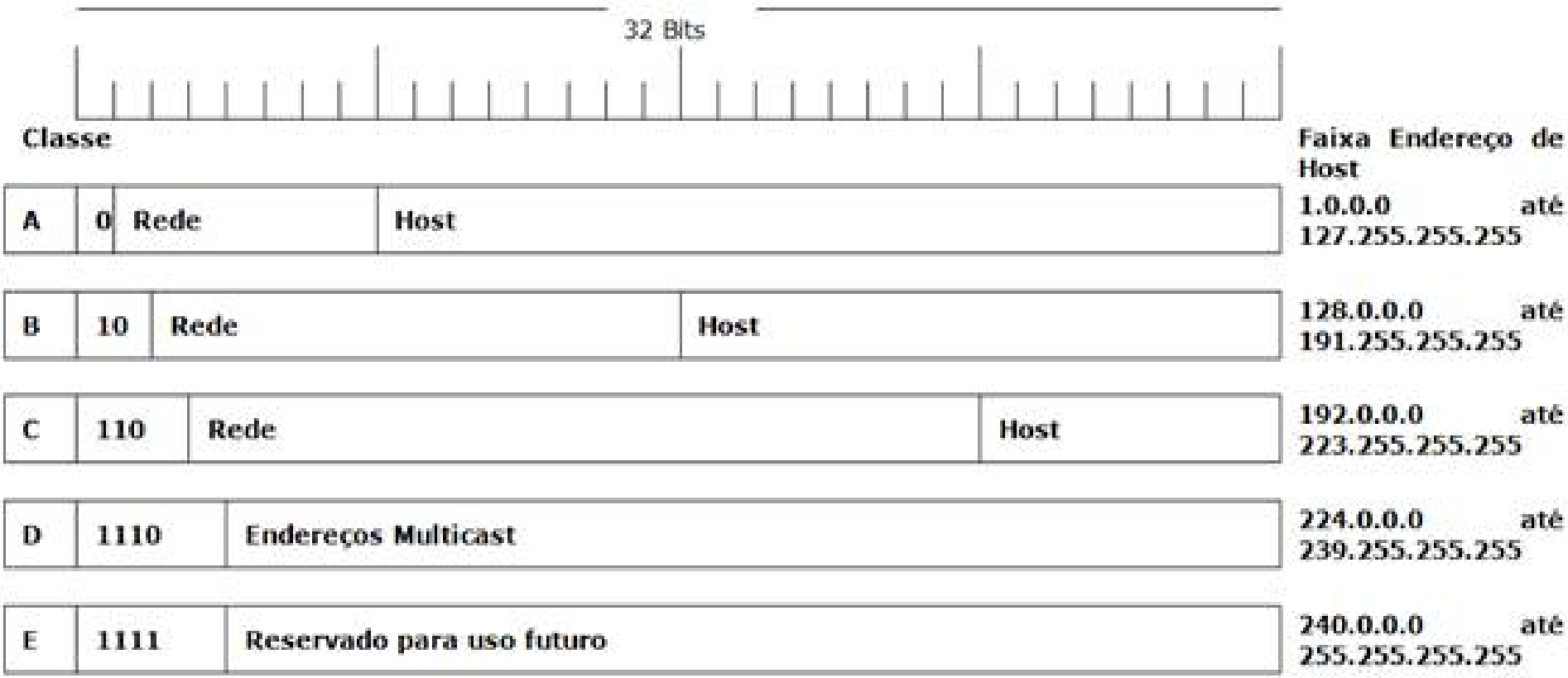
- **Netid** é o conjunto de bits, o prefixo, que representa a rede;
- **Hostid** é o conjunto de bits que representa a máquina dentro da rede.

Exemplo :

(n representa Netid e h representa Hostid)

Estrutura do IP: nnnnnnnn.nnnnnnnn.nnnnnnnn./hhhhhhhhh

Classes de Endereços IP



Máscara de rede

O conceito de mascara de rede é utilizado para a identificação, no endereço, dos bits que são Netids e dos que são Hostids.

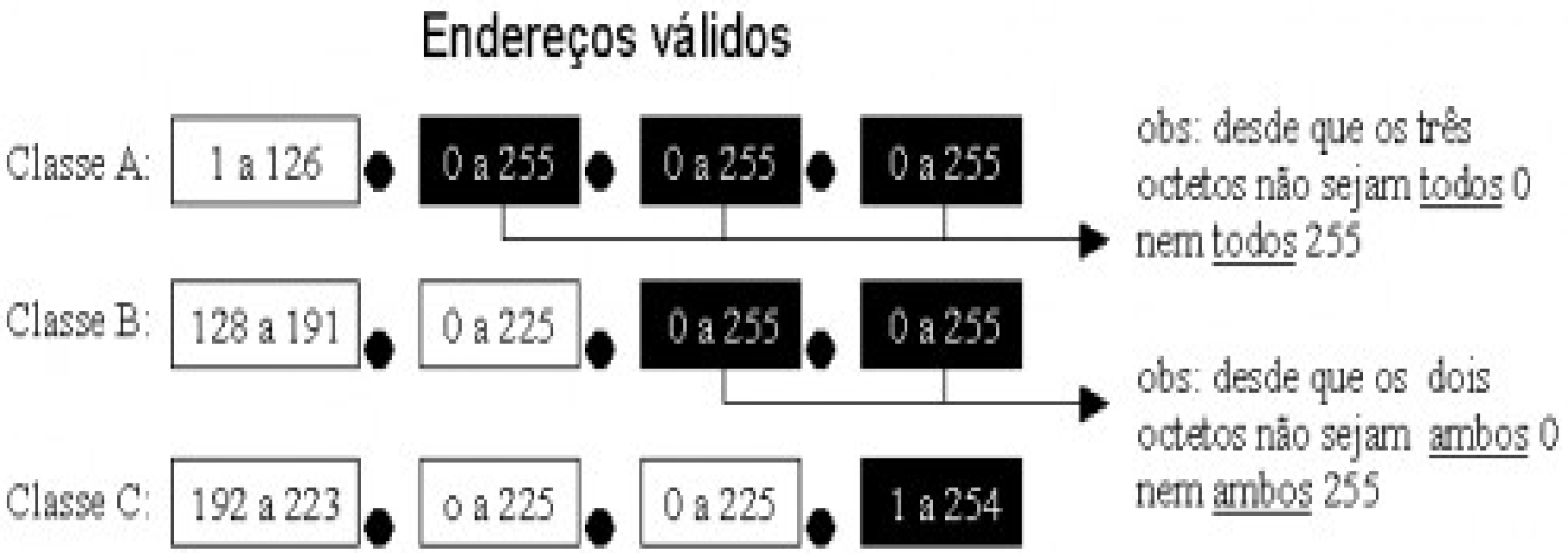
- Bits que assumem o valor 1 são Netid;
- Bits que assumem o valor 0 são Hostid.

Exemplo:

255.255.255.0 – 11111111.11111111..11111111.00000000

Máscara de Rede para as Classes

- Classe A – 255.0.0.0
- Classe B – 255.255.0.0
- Classe C – 255.255.255.0



Endereços especiais

- **Loopback –** Endereço utilizado para comunicação interna à interface, (host com o próprio host), e que assum o valor 127.0.0.1;
- **Endereço de Rede:** Endereços IP que têm todos os bits de Hostid assumindo valor 0;
- **Broadcast:** Endereços IP que têm todos os bits de Hostid assumindo valor 1;
- **Rota Default:** Endereço para o qual são enviados os pacotes cujos destinos não são pertencentes à rede do emissor. Normalmente a Rota Default é representada pelo endereço 0.0.0.0

Classles Inter Domain Routing - CIDR

Sub-redes – Redes fisicas cujos endereços são um subconjunto de um conjunto de endereços IP (Cl. A, B, ou C);

Motivação

Com a explosão da Internet e o uso não escalonavel de alocação em classes, surgiram problemas como: Exaustão de endereços de Classe B, Explosão da tabela de roteamento, Exaustão de endereços.

Dados gerais sobre Segurança de Redes

Segurança

"…a segurança se preocupa em garantir que pessoas mal-intencionadas não **leiam** ou, pior ainda, **modifiquem** secretamente mensagens enviadas a outros destinatários. Outra preocupação da segurança são as pessoas que tentam ter acesso a **serviços remotos** que elas **não estão autorizadas** a usar. Ela também lida com meios para saber se uma mensagem supostamente verdadeira é um **trote**. A segurança trata de situações em que mensagens legítimas são **capturadas** e **reproduzidas**, além de lidar com pessoas que tentam **negar o fato** de terem enviado determinadas mensagens.

A maior parte dos problemas de segurança é causada intencionalmente por pessoas maliciosas que tentam obter algum benefício, chamar a atenção ou prejudicar alguém. "

Andrew Stuart Tanenbaum – Redes de computadores 4º Edição.

Introdução

A Segurança de redes envolve conhecimentos de diversos áreas, como:

- Administração de Sistemas;
- Sistemas Operacionais;
- Sistemas de Arquivos;
- Protocolos de Redes.

5 Principios norteadores

Um ambiente seguro, prioritariamente, deve atender 3 requisitos básicos, conhecidos como CID:

- **C**onfidencialidade;
- **I**ntegridade;
- **D**isponibilidade;

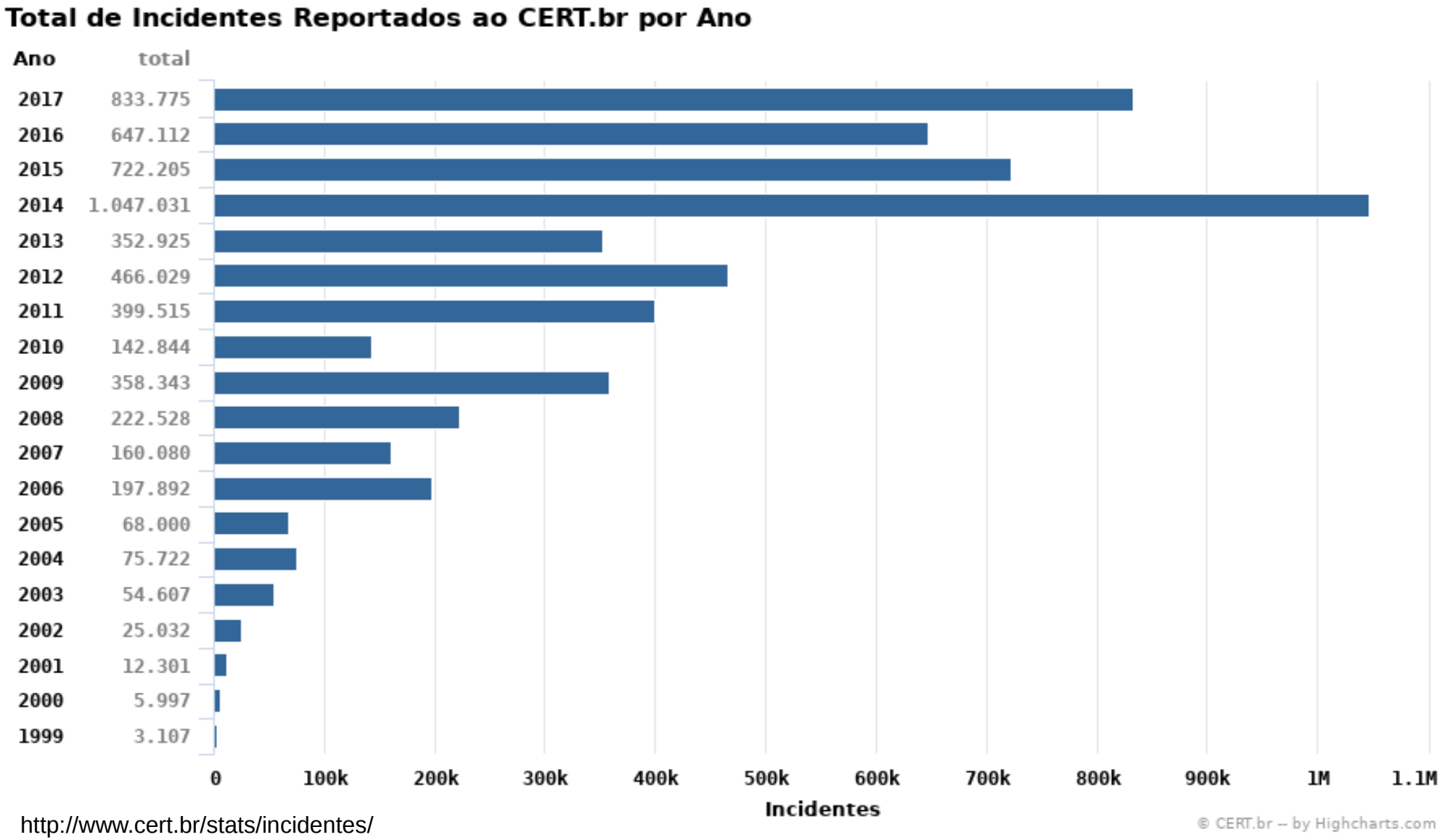
Em complemento a isso, temos outros dois requisitos, que se apresentam com a mesma importância do CID, contudo, menos discutidos, mas não menos importantes.

- Não repúdio;
- Autenticidade.

Incidentes reportados até 2017

cert.br
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

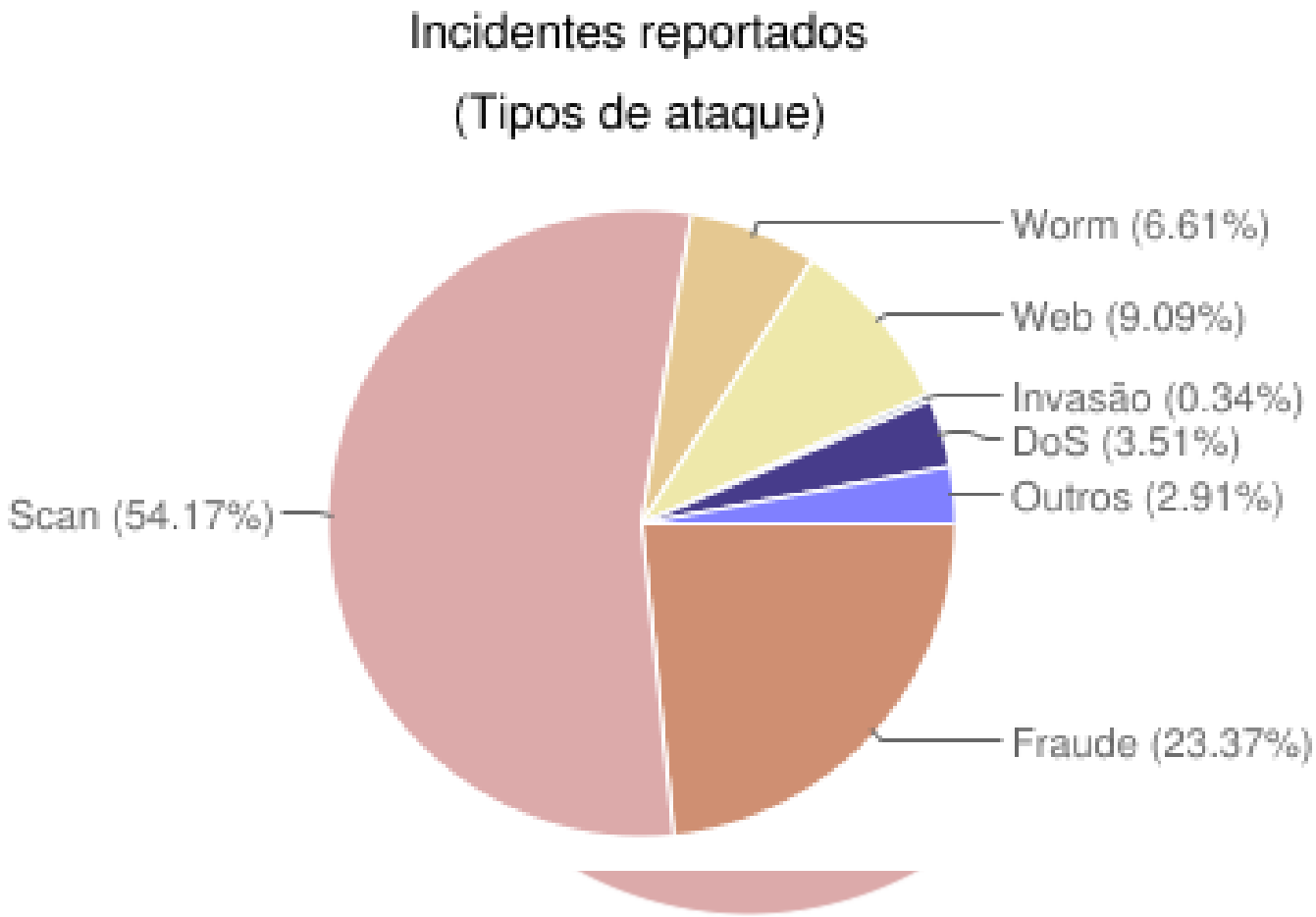
Valores acumulados: 1999 a 2017 novo



http://www.cert.br/stats/incidentes/

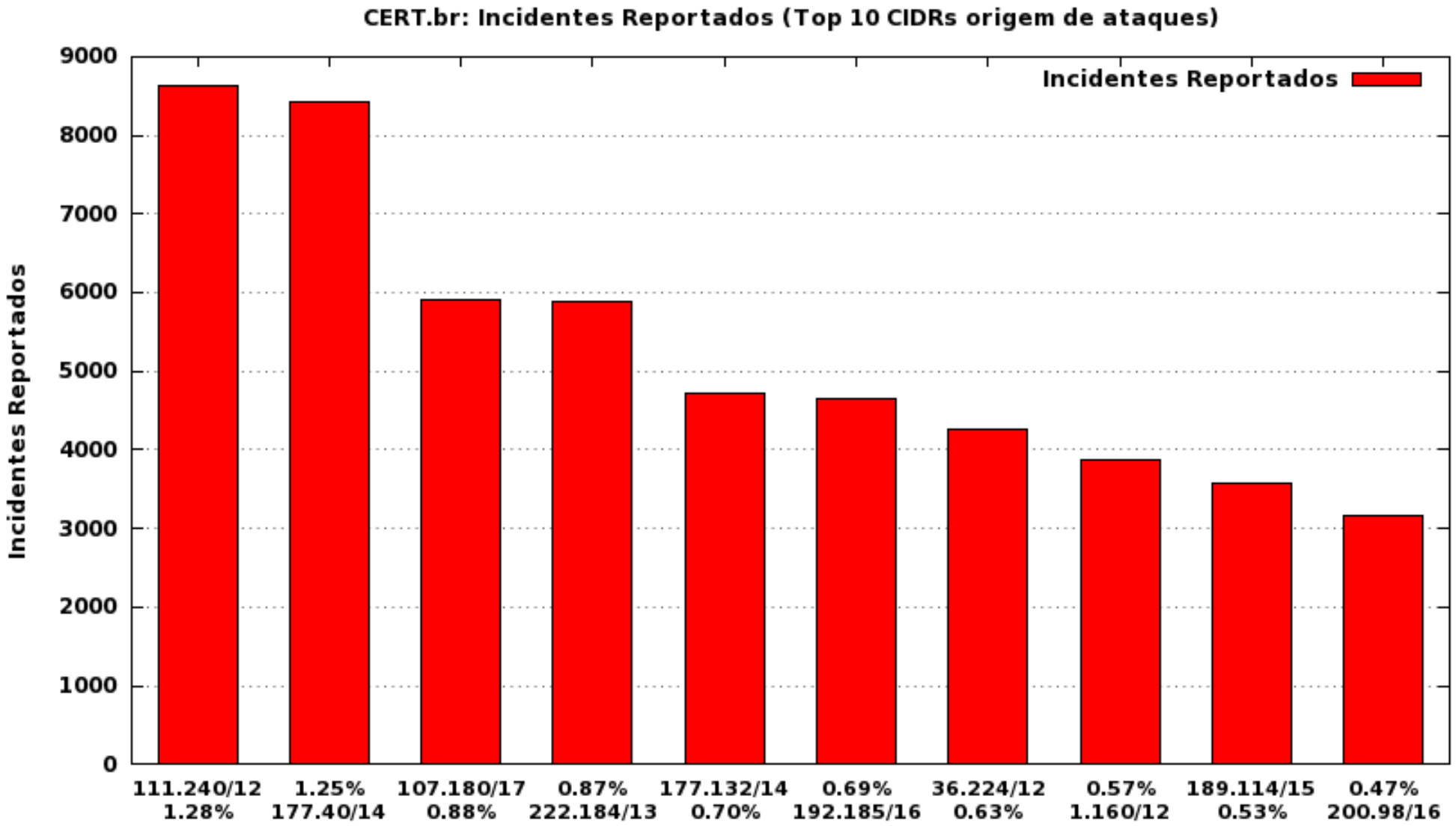
Incidentes por tipo de ataque

Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2017



http://www.cert.br/stats/incidentes/

Incidentes por CIDR - 2015



http://www.cert.br/stats/incidentes/

Panorama Global

Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2017

Tabela: Totais Mensais e Anual Classificados por Tipo de Ataque.

Mês	Total	worm (%)		dos (%)		invasão (%)		web (%)		**scan** (%)		**fraude** (%)		outros (%)	
jan	**64161**	1119	1	154	0	62	0	12169	18	44475	69	5424	8	758	1
fev	**27092**	1469	5	76	0	35	0	4362	16	16809	62	3815	14	526	1
mar	**54305**	1391	2	19	0	23	0	6281	11	41423	76	4587	8	581	1
abr	**51011**	2086	4	29	0	18	0	7782	15	35530	69	5310	10	256	0
mai	**47616**	2100	4	8	0	50	0	6232	13	32858	69	6027	12	341	0
jun	**49519**	3949	7	237	0	14	0	8320	16	30959	62	5733	11	307	0
jul	**257618**	4973	1	207780	80	1	0	4131	1	34364	13	5559	2	810	0
ago	**54035**	4110	7	11314	20	23	0	3037	5	28592	52	6513	12	446	0
set	**47940**	7264	15	254	0	24	0	1465	3	35474	74	3308	6	151	0
out	**74116**	7350	9	184	0	13	0	1691	2	60890	82	3690	4	298	0
nov	**63646**	5253	8	120	0	39	0	3245	5	51466	80	3316	5	207	0
dez	**42716**	4037	9	13	0	99	0	2051	4	30418	71	6037	14	61	0
Total	**833775**	45101	5	220188	26	401	0	60766	7	443258	53	59319	7	4742	0

Legenda

worm: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.

dos (DoS -- Denial of Service): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.

invasão: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.

web: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.

scan: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.

fraude: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.

outros: notificações de incidentes que não se enquadram nas categorias anteriores.

Obs.: Vale lembrar que não se deve confundir scan com scam. Scams (com "m") são quaisquer esquemas para enganar um usuário, geralmente, com finalidade de obter vantagens financeiras. Ataques deste tipo são enquadrados na categoria fraude.

Boa noite!