**Tópicos Avançados de Redes**

* **BYOD**

O conceito de trazer o próprio dispositivo*(Bring Your Own Device*, BYOD), acessar qualquer conteúdo em qualquer forma é uma forte tendência que exige mudanças significativas. Com o BYOD os usuários têm liberdade de usar dispositivos pessoais para acessar informações e se comunicar em uma rede pública ou privada. Com o aumento da oferta dos dispositivos a custos acessíveis, funcionários, alunos e pessoas de um modo geral podem ter computadores e dispositivos de rede para uso pessoal. O BYOD significa qualquer dispositivo, qualquer propriedade, usado em qualquer lugar. Como isso afeta a topologia, arquiteturas e outras coisas?

* **Colaboração e vídeo**

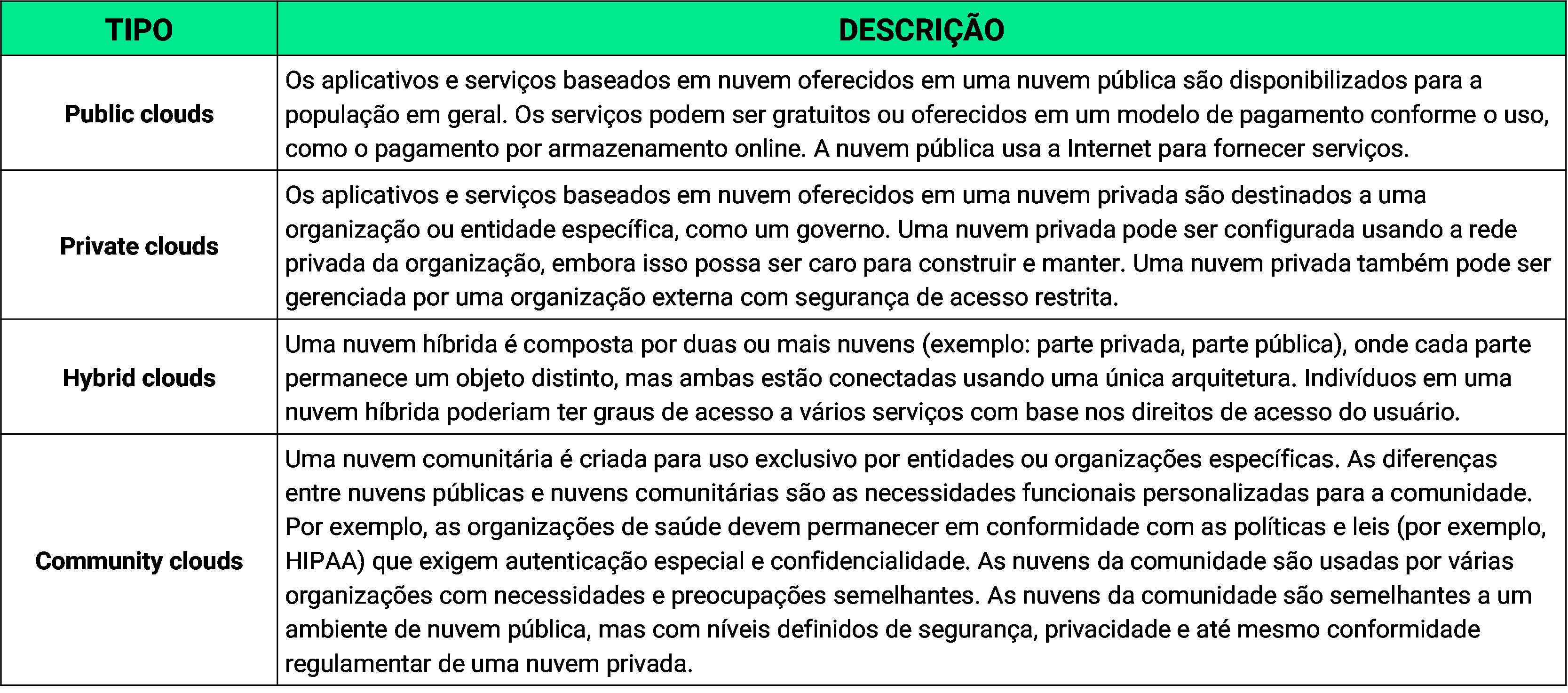
Os indivíduos se conectam à rede não apenas para acessar a Internet ou aplicativos, mas também para trabalhos colaborativos uns com os outros. O conceito da colaboração é uma prioridade crítica e estratégica que as organizações usam para se manterem competitivas. É também uma prioridade na educação. Outra questão que é crítica para a comunicação e colaboração é o tráfego de vídeo na rede. O vídeo é usado para comunicação, colaboração e entretenimento. As vídeo-chamadas são feitas por qualquer pessoa com acesso à Internet. A videoconferência é um recurso poderoso para se comunicar tanto para fins de corporativos quanto pessoais. Aplicações em tempo real, como telefonia e videoconferência, têm requisitos estritos de atraso.

* ***Cloud computing***

Muitas empresas de comércio na Internet  estão rodando suas aplicações na “nuvem” — como na EC2 da Amazon, na Application Engine da Google ou na Azure da Microsoft. Diversas empresas e universidades também migraram suas aplicações da Internet (por exemplo, e-mail e hospedagem de páginas Web) para a nuvem. Empresas de nuvem não apenas oferecem ambientes de computação e armazenamento escaláveis às aplicações, mas também oferecem acesso implícito às suas redes privativas de alto desempenho.

A computação em nuvem é uma das formas de acessar e armazenar dados como um serviço. A computação em nuvem permite armazenar arquivos de clientes corporativos e pessoais e fazer *backup* de uma unidade inteira em servidores através da Internet. Aplicativos como editor de texto e de fotos podem ser acessados ​​na nuvem. Para as organizações (e corporações) a computação em nuvem estende os recursos de TI sem requerer investimentos em nova infraestrutura, treinamento de novos funcionários ou licenciamento de novo *software*. Os serviços em nuvem estão disponíveis sob demanda e oferecidos de forma econômica para qualquer empresa e dispositivo que estejam em qualquer lugar do mundo, sem comprometer a segurança ou a função. Os serviços em nuvem são possíveis por causa dos *data centers* que são instalações usadas para hospedar sistemas computacionais e componentes associados. Um *data center* pode ocupar desde uma sala de um edifício até um campus.

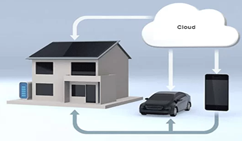
Os *data centers* têm custos de construção, implantação e manutenção. Por isso as grandes organizações têm condições de usarem *data centers* construídos de forma privada para armazenar seus dados e fornecer serviços aos usuários. As organizações menores podem reduzir o custo geral de propriedade (*total cost of ownership*, TCO) ao alugar servidores e serviços de armazenamento de uma organização maior de *data center* na nuvem. Para segurança, confiabilidade e tolerância a falhas os provedores de serviços de nuvem normalmente armazenam dados em *data centers* distribuídos. A Tabela a seguir descreve os tipos de nuvem.



* **Outros aspectos de rede**

*Smart Home:*

As tendências em rede não afetam somente a maneira como nos comunicamos nos ambientes de trabalho e escolar, mas também mudam muitos aspectos em nossa casa. As novas tendências para as casas incluem “tecnologia de casa inteligente”. As *smart homes* integram os eletrodomésticos e sistemas do dia a dia que podem se comunicar com outros dispositivos para torná-los mais inteligentes ou automatizados. A tecnologia da casa inteligente se torna mais comum à medida que as tecnologias de rede doméstica e internet se expandem. A Figura a seguir ilustra um exemplo de casa inteligente.



*Powerline:*

A rede *Powerline* para redes residenciais utiliza a fiação elétrica existente para conectar dispositivos. Usa um adaptador *powerline* padrão que permite que dispositivos se conectem à LAN onde há uma tomada elétrica. Nenhum cabo necessita ser instalado e pouca ou nenhuma energia elétrica adicional é utilizada. A rede *Powerline* é útil, por exemplo, quando o acesso sem fio não consegue atingir todos os dispositivos da casa. Não substitui o cabeamento dedicado em redes, mas é uma alternativa quando os cabos de rede ou a comunicação sem fio não são possíveis ou eficazes.

*Wireless Broadband:*

Em áreas onde o cabo (metálico ou óptico) e o DSL (*Digital Subscriber Line*) ou GPON (*Gigabit Passive Optical Network*) não estão disponíveis a conexão sem fio pode ser utilizada para se conectar à Internet. Um provedor de serviços de Internet sem fio (WISP) é um ISP que conecta assinantes a um ponto de acesso designado ao usar tecnologias sem fio semelhantes a encontradas em redes locais sem fio domésticas (WLANs). Os WISPs são mais comuns em ambientes rurais onde os serviços DSL/GPON ou a cabo não estão disponíveis. Da perspectiva do usuário doméstico a utilização não é muito diferente do serviço DSL/GPON ou a cabo. A principal diferença é que a conexão da casa para o ISP é sem fio em vez de um cabo físico.

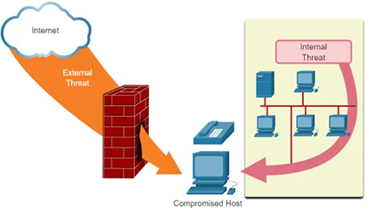
* **Segurança**

*Ameaças:*

Uma maneira de agrupar as ameaças é em termos de ataques passivos e ativos. Os ataques passivos incluem espionagem do tráfego da rede entre o navegador e o servidor, e obtenção de acesso a informações em um *Website* que deveria ser restrito. Os ataques ativos incluem personificação de outro usuário, alteração de mensagens em trânsito entre o cliente e o servidor, e alteração de informações em um *Website*. Outra maneira de classificar as ameaças de segurança na Web é em termos do local da ameaça: o servidor Web, o navegador Web e o tráfego de rede entre o navegador e o servidor. As questões de segurança de servidor e navegador entram na categoria de segurança do sistema de computador.

* Vírus, *worms* e cavalos de Tróia: contêm *software* ou código malicioso em execução no dispositivo do usuário.
* *Spyware* e *adware*: são tipos de *software* instalados no dispositivo do usuário. O *software* então coleta secretamente informações sobre o usuário.
* Ataques *zero-day*: também chamados de ataques de hora zero, ocorrem no primeiro dia em que uma vulnerabilidade se torna conhecida.
* Ataques de agentes: uma pessoa mal-intencionada ataca os dispositivos do usuário ou recursos de rede.
* Ataques de negação de serviço (*Denial of Service*, DoS): tais ataques tornam mais lento ou bloqueiam aplicativos e processos em um dispositivo de rede.
* Interceptação e roubo de dados: este ataque captura informações privadas da rede de uma organização.
* Roubo de identidade: este ataque rouba as credenciais de *login* de um usuário para acessar dados privados.

A Figura a seguir mostra um exemplo de ameaças à segurança.



*Soluções:*

Para uma rede doméstica:

* Antivírus e *antispyware*: tais aplicativos ajudam a proteger os dispositivos finais de serem infectados com *software* malicioso.
* Filtragem de *firewall*: bloqueia o acesso não autorizado da rede.

Para redes maiores:

* Sistemas de *firewall* dedicados: proveem recursos de*firewall* mais avançados que podem filtrar grandes quantidades de tráfego com mais eficiência.
* Listas de controle de acesso (ACL): controlam o acesso e o encaminhamento de tráfego com base em endereços IP e aplicativos.
* Sistemas de prevenção de intrusão (IPS): identificam ameaças que se propagam rapidamente, como ataques de dia zero ou hora zero.
* Redes virtuais privadas (VPN): proveem acesso seguro a uma organização (corporação) para funcionários remotos.