Комп'ютерні мережі

Потреби офісу або комплексу в комп'ютерній мережі дуже специфічні і залежать від бюджету, розміру, потужності та загальних оперативних потреб установи. Агентствам слід розглянути можливість найму спеціального IT-спеціаліста та мережевого персоналу для підтримки створення офісних та суб-офісних мереж.

Облаштування офісу/комплексу

У більшості польових локацій буде використовуватися поєднання декількох найсучасніших офісних мережевих пристроїв. Ці елементи можуть включати:

Підключення до зовнішнього постачальника послуг Інтернету (ISP)– Підключення до зовнішнього постачальника послуг Інтернету може здійснюватися за допомогою супутникового Інтернету, телефонної лінії або іншої форми виділеного підключення до мережі, підтвердженої провайдером.

Модем – Модеми приймають сигнали, що надходять від провайдерів, і перетворюють їх у сигнали, придатні для використання в домашніх або офісних мережах. Модеми також містять інформацію про користувача, яка використовується для ідентифікації, відстеження та моніторингу трафіку з метою безпеки та виставлення рахунків. Без модему будь-яке домашнє або офісне мережеве обладнання не зможе спілкуватися із зовнішніми мережами.

Маршрутизатор (роутер) – Маршрутизатор - це пристрій, який розділяє і управляє інтернет-трафіком, дозволяючи декільком комп'ютерним пристроям мати свої власні унікальні IP і MAC-адреси і одночасно спілкуватися з інтернетом і один з одним по мережі. Маршрутизатори мають різноманітні конфігурації та функції. Деякі з них можуть відстежувати і контролювати трафік у локальній мережі, а інші мають можливість підключення до Wi-Fi. Тип використовуваного маршрутизатора буде залежати від операційних потреб.

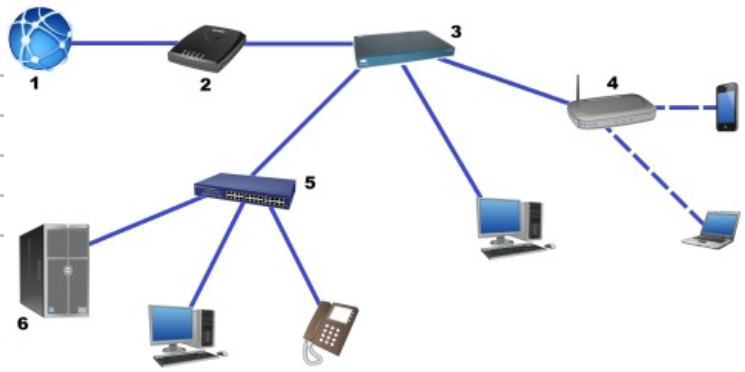
Брандмауер – це будь-який пристрій, який спеціально відстежує і фільтрує інтернет-контент, що надходить із зовнішніх мереж. Брандмауери корисні для запобігання шкідливому програмному забезпеченню, випадковому несанкціонованому вторгненню в мережу або навіть для блокування контенту, не дозволеного IT-політикою окремих організацій. У спрощених мережах брандмауери часто об'єднані з модемами або маршрутизаторами, але просунуті мережі можуть мати окремі брандмауери, які мають різні протоколи для різних користувачів сервісу.

Мережевий комутатор – Мережевий комутатор є вдосконаленою формою маршрутизатора - він контролює і розподіляє інтернет між декількома мережевими пристроями, проте комутатори здатні до детального моніторингу та управління аж до рівня окремого пристрою. Комутатори також використовуються для фільтрації, блокування та захисту внутрішніх мереж, подібно до брандмауерів, що захищають від зовнішніх загроз.

Сервер – Серверами називаються комп'ютери, які повністю призначені для зберігання та обміну файлами в мережі. Сервери можуть бути як простими, як звичайні настільні комп'ютери, так і складними, як великі спеціалізовані обчислювальні пристрої, що мають особливі вимоги до встановлення. Останніми роками багато установ почали використовувати «віддалені» сервери, на яких розміщуються файли та дані, а також керують ними з місць за межами офісів, іноді з інших країн. Винесені сервери є цілком

прийнятним рішенням, однак, якщо користувачі сервера мають нестабільне з'єднання з Інтернетом, локалізований сервер може бути кращим.

1	Зовнішній інтернет-провайдер
2	Модем
3	Маршрутизатор/Брандмауер
4	Wi-Fi роутер
5	Мережевий комутатор
6	Сервер



Операційна безпека

Вимоги до операційної безпеки кожної з локальних мереж повинні відповідати основним правилам.

Контроль доступу –Доступ до мереж та обчислювальних пристроїв повинні мати тільки авторизовані особи. Всі комп'ютери повинні бути захищені паролем, а WI FI роутери також повинні вимагати введення облікових даних. Деякі мережі дозволяють тимчасовий гостьовий доступ, однак потреби в спеціальних налаштуваннях варіюються залежно від операційного середовища.

Шкідливе програмне забезпечення – Всі комп'ютерні пристрої в мережі повинні мати певну форму антивірусного програмного забезпечення, а операційні системи завжди повинні бути оновленими. Установам слід розглянути можливість встановлення брандмауерів та/або комутаторів з керованими налаштуваннями, щоб також зменшити кількість спроб вторгнення або передачі шкідливого програмного забезпечення.

IT-політика – Агенції повинні розробити та поширити внутрішню IT-політику для всіх співробітників та користувачів мережі. IT-політики повинні включати правила та норми щодо того, що вважається прийнятною поведінкою, які правила використання різних типів обладнання, а також встановлювати вказівки щодо недотримання цих правил.