Computer Networking

The computer networking needs of an office or compound are very specific to the budgets, the size, the capacity, and the overall operational needs of the agency. Agencies should investigate hiring dedicated IT and networking staff to support setting up office and sub office networks.

Office/Compound Set Up

In most field locations, there will be a mix of several very coming office network equipment. These items might include:

Connection to External ISP – Connection to an external Internet Service Provider (ISP) may come in the form of satellite internet, telephone line, or some other form of dedicated connection to a grid proved by the ISP.

Modem – Modems receive signals coming from ISPs and translate them into usable signals by home or office networks. Modems also contain user specific information which is used to identify, trace and monitor traffic for security and billing purposes. Without a modem, any home or office based networking equipment would be incapable of actually speaking to outside networks.

Router – A Router is a device that splits and manages internet traffic, enabling multiple computing devices to have their own unique IP and MAC addresses, and communicate with the internet and each other at the same time over a network. Routers have a variety of configurations and functions. Some can monitor and control traffic on the local network, and others have wifi capability. The type of router used will depend on the operational needs.

Firewall – A firewall is any device that specifically monitors and filters internet content coming from outside networks. Firewalls are useful for preventing malicious software, casual unauthorised intrusion into networks, or even block content not allowed by the IT policy of individual organisations. In simplified networks, firewalls are often merged with modems or routers, but advanced networks can have standalone firewalls that have different protocols for different users of the service.

Switch – A network switch is like an advanced form of a router – it controls and distributes the internet between multiple networked devices, however switches are capable of detailed monitoring and control down to the individual device level. Switches are also used to filter, block and secure internal networks similar to firewalls securing external threats.

Server – Servers are defined a computers that are fully dedicated to storing and sharing files within a network. Servers can be as simple as regular desktop computers, or as complex as large specialised computing devices that have special installation requirements. In recent years, many agencies have started using “offsite” servers, which host and manage files and data from locations outside of offices, sometimes from a different country. Offsite servers perfectly acceptable solutions, however if the users of the server have inconsistent connection to the internet, a localised server may be preferable.

1	External ISP
2	Modem
3	Router/Firewall
4	Wi-Fi Router
5	Network Switch
6	Server

Operational Security

The operational security requirements of each of local networks should follow basic rules.

Access Control – Only authorised persons should have access to networks and computing devices. All computers should be password protected, and wifi routers should also require a login credentials. Some networks allow for temporary guest access, however the needs for special settings vary depending on the operational environment.

Malicious Software – All computing devices on networks should have some form of anti-virus software, and operating systems should always be up to date. Agencies should consider installing firewalls and/or switches with managed settings to also cut back on the intrusion attempts or the transmission of malicious software.

IT Policy – Agencies should develop and share internal IT policies for all employees and users of the network. IT policies should include rules and regulations for what is considered acceptable behaviour, what he rules for using different types of hardware is, and establish guidelines for failure to comply.