Public Spot

A Public Spot controls the provision of Internet access in areas with temporary users. A typical example is a wireless LAN, which potentially allows any client to connect directly to the Internet. To prevent this and maintain control over Internet access, a Public Spot is an instance at which users are required to authenticate themselves before they can access the Internet.

Applications

A Public Spot can be employed in various scenarios. A typical example is in hotels, where a hotel operator wishes to offer his guests time-dependent Internet access, which could also be billed accordingly. At the same time, he also wants to prevent access by unauthorized persons. Another example is a company that offers Internet over Wi-Fi to its guests, but also wants to prevent outsiders from using it.

Note that the capabilities of the Public Spot Option depend upon the device on which it is activated. If it is operated on an individual access point (Fig. 1), the Public Spot can only manage the access of WLAN clients which associate directly with this access point. In contrast, a router (Fig. 2), central site VPN gateway, and WLAN controller can—through the Public Spot—provide authentication for an entire IP network, including multiple access points and their Wi-Fi clients or Ethernet clients. A WLAN controller (Fig. 3) can additionally manage the individual access points within the network. The WLAN controller distributes the configuration parameters to the access points automatically, so there is no need to configure the devices individually.

Also, Layer 3 tunneling enables the Public Spot to be operated even across WAN boundaries. Further information on Layer 3 tunneling can be found in the LCOS reference manual which is available for download free of charge on the LANCOM website.

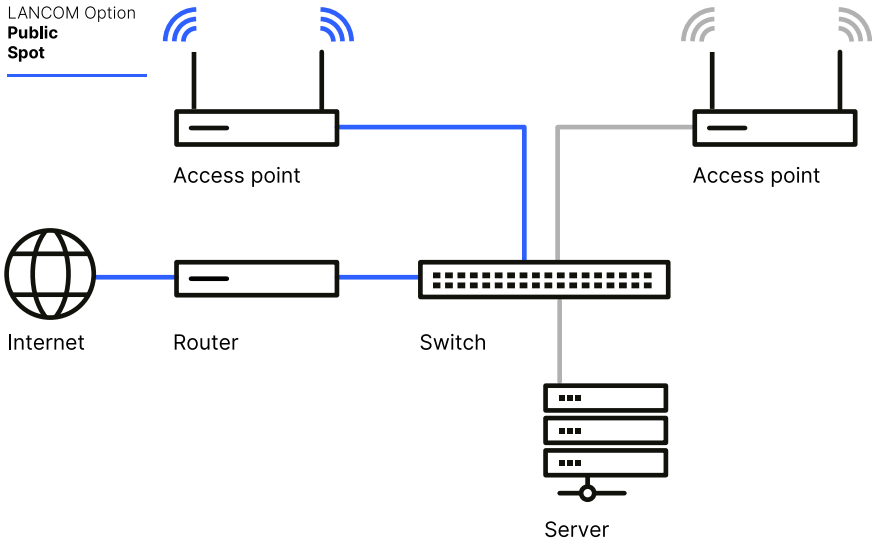

Figure 1:
Access point with
Public Spot Option

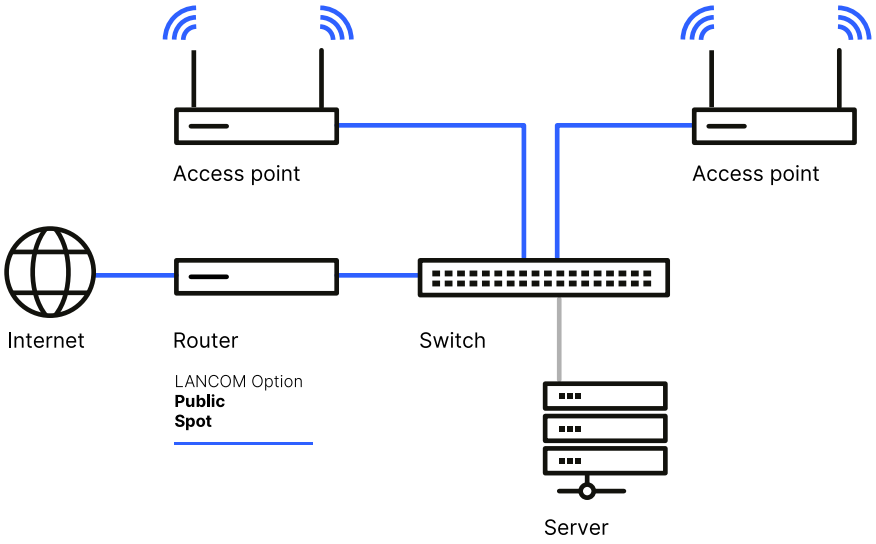

Figure 2:
Router with
Public Spot Option

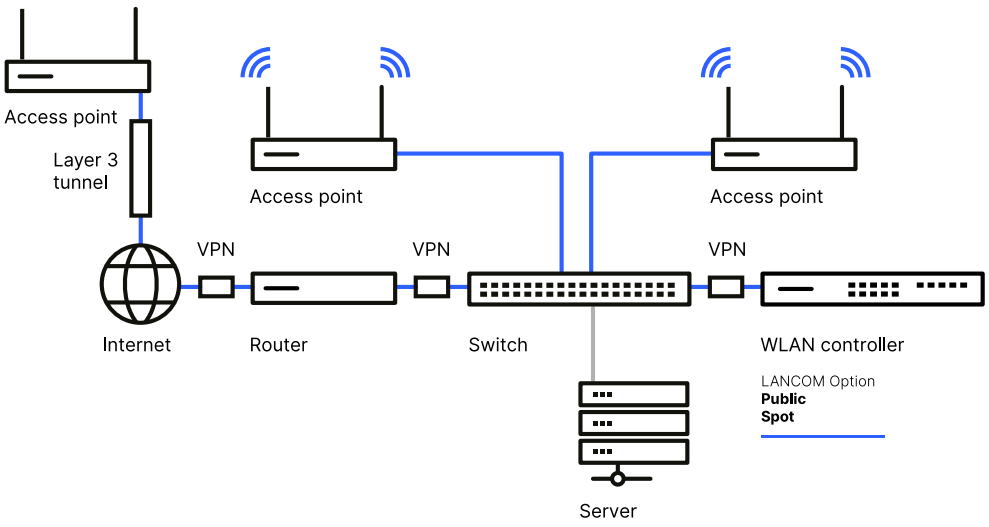

Figure 3:
WLAN controller with
Public Spot Option

Security

The subject of security in relation to Public Spots can be divided into four groups: separating the Public Spot network from the internal network, authentication, authorization, and accounting (AAA).

The first important aspect about security is the separation of the Public Spot from internal services and data. Separation can be achieved with the operation of VLANs (Virtual Local Area Networks), which allows the existing infrastructure to be used further on. As the name suggests, the VLAN itself is a separate virtual LAN with its own IP address range. Direct communication between the different VLANs is impossible. An additional option for separating the networks is to use Layer 3 tunneling. Here, an SSID on an access point is routed directly into a layer 3 tunnel. Data from an access point is not fed directly into a VLAN, but initially to a WLAN controller, which then, in turn, routes the data into the VLAN. The advantage of this is that only the network infrastructure behind the WLAN controller has to be VLAN-capable. Also, an existing VLAN configuration between the access point and WLAN controller does not require reconfiguration. This configuration also allows the Public Spot to operate over different WAN connections, assuming that the access point can obtain a profile from the WLAN controller.

Authentication at the Public Spot can be realized in various different ways. The conventional method uses a user name and password to authenticate at the Public Spot. Users require access credentials which they enter into a web login page before they can access the Internet. This login web page can be customized by the operator, for example to display the terms and conditions for using the hotspot.

The option of performing authentication by means of user name, password, and MAC address is used only rarely. This is desirable were the access credentials have to be used in combination with a specific end device only. The necessary authentication data is stored on a RADIUS server, which can be located externally, or it can be the device's own internal RADIUS server (authentication). The application itself runs on a browser operating HTTPS for security, ensuring that user information cannot be intercepted and misused.

When specifying the time frame, the hotspot operator can decide whether Internet access is valid for a certain period of time after the initial activation, or whether a set time budget is to be consumed incrementally (Fig. 4). The time information and the access credentials can be printed out on a voucher and handed over to the customer.

In addition, it is possible to provide internal and any number of external web pages in a so-called „walled garden“, access which does not require authentication at the Public Spot. For example, a hotel can provide access to web sites with information about the attractions to which it organizes day trips.

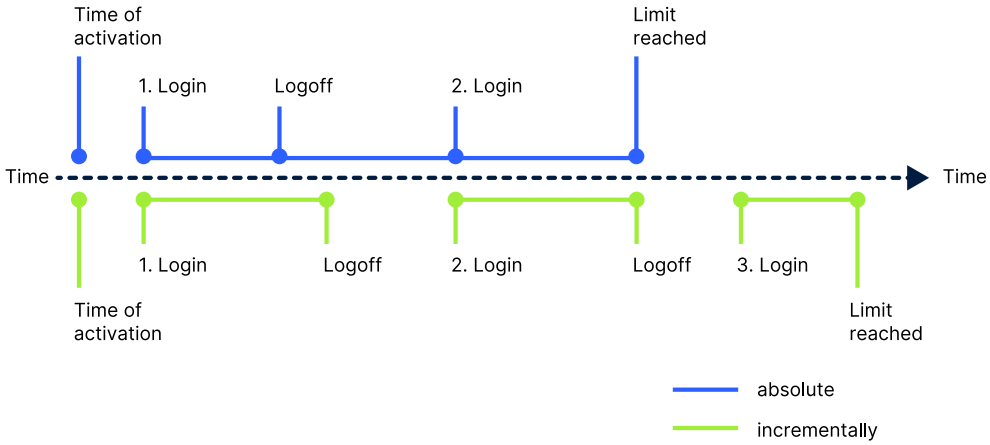

Figure 4:
Absolute and incremental Internet access limits

Logging and Filtering

It is also possible to record the login and logout activities of any Public Spot user. The MAC address used at the login is also saved. Furthermore, the start of each IP session can be logged. This information can be output by SYSLOG (accounting).

Yet another option is the use of web content filtering. Two different mechanisms are available here. One method relies on the stateful packet inspection firewall, which can, for example, block ports and prevent the connection to certain services. A second option is to operate a Content Filter, which uses category profiles to control access to web sites (HTTP and HTTPS).

Summary

The LANCOM Public Spot is a versatile and secure solution for scenarios in which guests and customers are provided with temporary Internet access, regardless if via wireless or cable.

LANCOM Systems GmbH
A Rohde & Schwarz Company
Adenauerstr. 20/B2
52146 Wuerselen | Germany
info@lancom.de | lancom-systems.com