ZONE MIGRATION IN NETWORK ACCESS

FIELD OF THE INVENTION

[0001] The present disclosure relates to the field of providing computer network access.

BACKGROUND

[0002] The use of laptop, cell phone, PDA and other mobile computing devices has become very common. Travelers, and particularly business travelers, expect and often require network access, such as access to the Internet, as they travel from one place to the next. Similarly, students in schools and doctors in hospitals require access throughout a their respective campuses or medical buildings. Even in a single venue, such as a hotel or conference center, travelers and guest desire network access at various locations throughout the venue including guest rooms, restaurants, meeting rooms, lobby, business centers, etc.

SUMMARY

[0003] The present disclosure is directed to providing a system for controlling network access in different physical locations of a network. In an embodiment, the disclosure describes a system for controlling access in a network for user moving between different physical locations of the network. For example, in an embodiment, when a user moves between different rooms in a particular venue, the system implements rules which establish when the user will be automatically authenticated to the new location, or whether a new authentication is necessary.

[0004] In an embodiment, network access is controlled by implementing different authentication rules for different network access points. A network access point is any wired or wireless connection point to a network. In an embodiment, a network access point is a wired or wireless port. Ports can include, for example, 802.1Q VLAN IDs or the like, TCP ports or the like, UDP ports or the like, and any other software defined communication endpoints. In an embodiment, a network access point is a physical connection to the network, such as, for example, an Ethernet jack, a phone jack, a wireless router, or the like.

An access point can also include any form of location identification, such as, for example, the triangulation of a wireless signal, the use of a global positioning system (GPS), or any other system for determining the location of a network user.

[0005] In an embodiment, access points are grouped into zones. In an embodiment, a zone includes one or more access points. In an embodiment, a network includes at least a plurality of zones. In an embodiment, a network administrator can configure access rules for allowing a user to move between access points within a zone and/or between zones. In an embodiment, for example, a user is allowed to move from access point to access point within a zone without having to re-authenticate. However, a user may be required to re-authenticate when moving between access points associated with different zones. This can be useful, for example, when a user is required to pay different amounts to access the network through access points in different zones or where different zones have different security levels associated with them. As used in the present specification, authentication can include, for example, a login, including a user name and/or password, the payment of a fee, the registration of a computer, entering a passcode or any other affirmative action taken by a user of a user device to gain permission to use a network.

[0006] For purposes of summarizing the disclosure, certain aspects, advantages and novel features of the inventions have been described herein. It is to be understood that not necessarily all such advantages can be achieved in accordance with any particular embodiment of the inventions disclosed herein. Thus, the inventions disclosed herein can be embodied or carried out in a manner that achieves or optimizes one advantage or group of advantages as taught herein without necessarily achieving other advantages as can be taught or suggested herein.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] The drawings are provided to illustrate embodiments of the inventions described herein and not to limit the scope thereof.

[0008] FIGURE 1 schematically illustrates an embodiment of a network.

[0009] FIGURE 2 illustrates a cross section of various access points in a hospitality setting.

[0010] FIGURE 3 schematically illustrates access points and network connections of various users in a conference setting.

[0011] FIGURE 4 illustrates an administrator setup screen for defining a plurality of access zones.

[0012] FIGURE 5 illustrates a flow chart of a decision tree for determining when a login is required to obtain network access in an embodiment.

[0013] FIGURE 6 illustrates a flow chart showing when a login is required when moving between different zones in an embodiment.

[0014] FIGURE 7 illustrates a timeline of two examples of users moving between different locations in a network.

DETAILED DESCRIPTION

[0015] FIG. 1 schematically illustrates an embodiment of a network access system. The system includes various user devices 141, 143, 145, 147, 149, 151, 153, 155. User devices can include, such as, for example, laptops, desktop computers, cell phones, PDAs and any other wired or wireless network enabled communication devices. The user devices 141, 143, 145, 147, 149, 151, 153, 155 communicate with access points 121, 123, 125, 127, 129. Access points 121, 123, 125, 127, 129 provide wired or wireless communications with network management device(s) 103. The network management device(s) 103 controls network communications in-between access points and between the access points and network 101. In an embodiment, the network management device(s) are operated by a single entity. In an embodiment, the network management device(s) create a single network. Optionally, intermediate network devices 105 can also be used, including, for example, routers, switches, hubs, repeaters, etc. to assist in providing communications between access points 121, 123, 125, 127 and network management device(s) 103. The network 101 can be, for example, a public network such as the Internet. Network management device(s) 103 can include network gateways, such as, for example, network access gateways commercially available from Nomadix, Inc. of Newbury Park, CA. As will be understood by those of skill in the art from the present disclosure, other network management devices can also be used. As illustrated in FIG. 1, the network includes three

different physical areas including lobby 107, conference center 109 and guest room 111. Each physical area includes one or more access points.

[0016] The network management device(s) 103 provide the ability to group the access points together for purposes of allowing a user device to move between certain access points without requiring re-authentication while requiring re-authentication when moving to other access points. The grouping of access points can be made, for example, along physical boundaries such as, for example, a wall. This can be done, for example, by allocating certain access points to a defined zone. In an embodiment, a zone is a room, group of rooms, building, group of buildings or the like. For example, the lobby 107 can be a first zone, the conference center 109 can be a second zone and the guest room 111 can be a third zone. In a simple example, a user device will be able to move between access points within a zone without having to re-authenticate, but will be required to re-authenticate when moving between access points located in different zones. Authentication, can include, for example, a login, payment of fees, a request for access, entry of a code, or any other action required by the user to request access to the network. In another example, a user device, once authenticated to the lobby zone 107 can be allowed to access the conference center zone 109 without reauthentication, but may be required to re-authenticate when moving to the guest room zone 111.

[0017] In an embodiment, access points advertise their presence by broadcasting a Service Set Identifier (SSID), Extended Service Set Identifier (ESSID), and/or Basic Service Set Identifier (BSSID), or the like, collectively referred to herein as SSID. In an embodiment, the same SSID is assigned to all access points and zones in a network. In an embodiment, a different SSID is assigned to each zone or to a group of zones. In an embodiment, multiple SSID's can be assigned to the same zone or same set of access points. In this respect virtual SSID's can be set up corresponding to different groupings of zones or access points. For example, at the same hotel or conference center, two different conferences which are simultaneously occurring can have custom SSID's corresponding to the access grated to each group. Conference A2 2009 for example can have a custom SSID entitled "Conference A2 2009" which allows access to access points in the Lobby, Guest Rooms and Meeting Rooms without re-authentication, but not in the Business Center. A second

conference, Conference B1 2009, can also have a custom SSID entitled "Conference B1 2009" which allows access to the Lobby, Meeting Rooms, Guest Rooms *and* the Business Center without re-authentication. Similarly, network providers can also have various levels of SSIDs allowing access to different groups of access points where multiple SSIDs correspond to the same access point or zone. Different SSIDs can correspond to different payment levels. For example, an inexpensive SSID access may only grant access to the Lobby, whereas a more expensive SSID can grant access to the Business Center or Meeting Rooms.

[0018] In an embodiment, an amount of bandwidth, or maximum bandwidth can be assigned to different access points, groups of access points, zones, groups of zones or custom SSIDs.

[0019] The following is a non-limiting example of Zone Migration. As used in this example, a zone is a group of VLAN IDs. When customers connect to the network, for example, at a hotel, they are authenticated in one of four zones:

Lobby/Restaurant/Common Area: 100-150

Guest Wired: 201-700

Guest Wireless: 801-1500

Meeting Room A: 1601-1700

Zone Migration provides the ability to the network to group the VLANS together, meaning that 100-150 would be grouped together, so the user could go from access point 101 in the lobby to access point 125 in the restaurant without being required to re-authenticate. A user would then be required to re-authenticate when moving between the Lobby and Meeting Room A.

[0020] FIG. 2 illustrates a cross section of various access points in a hospitality setting. Hotel 201 includes guest rooms 203, conference room 205, restaurant 207 and lobby 209. The guest rooms 203, conference room 205, restaurant 207 and lobby 209 include various access points 221. Although illustrated as having one or more access points in each room, it is to be understood that fewer or more access points can be used. For example, in an embodiment, a single access point can be used for multiple guest rooms. The access points can be configured into various zones. The zones can be defined along room lines or in any

other configuration. For example, the access points 221 in the guest rooms 203 area can all be a single zone. Alternatively, access points 221 on a single floor or across less than all floors can also be configured into a zone. As will be understood by a person of skill in the art, zones can be defined along any desired physical locations, incorporating the access points in those physical zones. As will also be understood by those of skill in the art, many different types of facilities will benefit from the present disclosure. For example, although described mainly with respect to hotels, other facilities can use the present access point zone system including schools, colleges, universities, hospitals, government buildings, businesses, or any other public or private networking systems. Also, zones do not need to be restricted to a particular building, but can include multiple buildings.

[0021] FIG. 3 schematically illustrates access points and network connections of various users in a conference setting. As illustrated, various user devices, are connected with, attempting to connect with, or are moving between connections with various access points. For example, user device 351 is wirelessly communicating with access point 321. User device 352 is attempting to access the network through access points 321, 323, 325, but has not yet been authenticated and thus is not able to send or receive communications over the network.

[0022] Devices are generally programmed to automatically select between access points, by, for example, determining which access point provides the strongest signal. User device 356 is in-between three different access points and is able to communicate with all of them, but will eventually choose one access point to communicate with. In some cases, an access point will not allow a device to communicate through it, in which case the user device will attempt to communicate with another the access point. For example, user device 357 may have the strongest signal with access point 325, but may only be authenticated with access point 337. In this case, the user devices will communicate with access point 337. Of course, as will be understood, user devices can be configured to select access points based on any number of different selection options, including, for example, signal strength, bandwidth availability, access rights, access points corresponding to a particular SSID, etc. When an access point is out of range, a user device will no longer be able to communicate with it and will attempt to find another access point. In an embodiment, switching between access points

is seamless, e.g. there is no loss of network session, and a user may not even realize that they have switched access points.

[0023] FIG. 4 illustrates an administrator setup screen for defining a plurality of access zones. The setup screen can be an independent computer program or it can run in a web browser. The setup screen provides the ability, as described above, to define zones which include multiple access points (labeled as "Ports-Locations" in FIG. 4). The zone setup information is stored in a database internal or external to the network management device(s) 103 and accessible to the network management device(s) 103. When a user attempts to access the network through an access point, the connection request is sent to the network management device(s) 103 which either allow the access request or deny it based on the programmed information in the database.

[0024] A relogin after migration selection 403 is provided to allow an administrator to determine whether to require a user to relogin after migrating between access points. An administrator can enter a zone name as desired in entry area 407. The administrator can then input the ports or locations that correspond to that zone in entry area 409. Optionally, an administrator can provide a description in entry area 411. The administrator can then determine whether a relogin (or reauthentication) will be required for moving between access points within the zone at selection 413. With relogin within zone 413 disabled, a user can freely move between access points without having to relogin. Add zone button 415 provides a subsequent screen which allows an administrator to define another zone. Reset button 417 allows an administrator to reset zone settings. Exising zones section 419 lists all previously defined zones for the network with corresponding ports or locations along with the relogin policy for each zone. To modify an existing zone, the administrator can click on the 'Edit' link of a particular zone. The fields at the top will then be populated with the attributes of the selected zone (name, ports, description and relogin policy). To remove a zone, the administrator can click on the 'Delete' link. A pop-up box will request the confirmation of the delete operation.

[0025] In an embodiment, zones cannot overlap, meaning that a port can belong to one and only one zone. In this embodiment, an error will be returned if the administrator enters a new zone that overlaps with an existing zone. In another embodiment, zones can be

configured to overlap such that the same port or access location can form part of two or more separate zones.

[0026] Many different zone to zone migration policies can be implemented, such as, for example, at the login Portal. In an embodiment, the network can be configured to (1) charge separately for each zone, or (2) allow free migration from "Zone 1" to "Zone 2" after accepting terms and conditions but require a payment when migrating from "Zone 2" to "Zone 1". Similarly, a single payment can be accepted for a group of zones, but an additional or separate charge could be required for other zones.

[0027] Zones can also be set up in other interfaces, such as, for example, command line interface (CLI) and simple network management protocol (SNMP). As would be understood by a person of ordinary skill in the art from the present disclosure, the various options and tools available in the interface embodiment of FIG. 4 can be mapped to CLI and SNMP interfaces.

[0028] In an embodiment, an unlimited number of zones can be configured. In an embodiment, the number of configurable zones is limited by the capacity of the network equipment used. For example, in an embodiment, up to 64 Zones or up to 32 Zones can be configured.

[0029] In an embodiment in which the number of zones is limited, if there is already the maximum number of Zones in the configuration, the network device will return a "Maximum number of Zones already reached" error.

[0030] In an embodiment, when a zone is added or modified by the administrator, the network device(s) will check for errors in, such as, for example, the zone name; the specified network access locations, such as, for example, the port assignments;

[0031] In an embodiment, the zone name is a string of a specified length, such as, for example, between 1 and 16 characters in length. In an embodiment, if this check fails, the network device(s) will return an"Invalid length of Zone Name" error; the zone description; and/or any other variables.

[0032] In an embodiment, the Zone Name must be unique. If this check fails, the network device(s) will return a "Zone Name already in use" error.

[0033] In an embodiment, the port name is a string of a specified length, such as, for example, between 1 and 128 characters in length (e.g., enough for at least 20 separate ports, or for at least 10 ranges of ports). The string can contain an individual numeric value (e.g., "211"), or a comma-separated list of numeric values (e.g., "211, 212"), or a range of numeric values with dash-separated delimiters (e.g., "111-799"), or a list of ranges of numeric values (e.g., "100-150, 201-700"), or a comma-separated list of individual numeric values and ranges (e.g., "211, 212, 213-651"). In an embodiment, if the string contains non-numeric values, the NSE will return a "Values may only be numeric, comma separated values or ranges" error.

[0034] In an embodiment, the numeric values cannot exceed 65535. When ranges are used, the right delimiter cannot be smaller than the left delimiter. In an embodiment, if these checks fail, the network management device will return an "Invalid format of Ports or value greater than 65535" error.

[0035] In an embodiment, ports of different zones cannot overlap. In an embodiment, if this check fails, the network devices will return a "Ports may not overlap ranges in other zones. Modify the overlapping zone first or change this entry" error. In an embodiment, ports are allowed to overlap and this check is not performed.

[0036] In an embodiment, the description is a string of specified length, such as, for example, between 0 and 128 characters in length. In an embodiment, if this check fails, the network device(s) will return an "Invalid length of Description" error.

[0037] In an embodiment, the relogin is a Boolean value in which no checking is necessary. In some WMI embodiments, the above errors will be shown in a pop-up error box, and in some embodiments, the field causing the error will simultaneously be highlighted with a red border.

[0038] There are a number of cases to consider when the zone (e.g. port in some embodiments) of the subscriber changes: (1) If the "Relogin after migration parameter" is disabled, the subscriber does not need to relogin; (2) If the "Relogin after migration parameter" is enabled, and no zone is specified, the subscriber will need to relogin; (3) If the "Relogin after migration parameter" is enabled, and one or more zones are specified, the

subscriber may need to relogin when: (1) the port changes to that of a different zone; or (2) the relogin policy of the zone is to require relogin.

[0039] In an embodiment, ports that do not belong to any of the configured zone are automatically assigned to a "default Zone". In an embodiment, the absence of a port is also assigned to a "default Zone". The relogin policy of the "default Zone" is simply derived from the "Relogin after migration" parameter. When the subscriber is re-logged in, and a portal is involved in the relogin process, the zone name will also be sent to the portal along with the other portal parameters (MAC address, room number, etc).

[0040] In an embodiment, the Administrator setup page also allows the administrator to set up SSID's corresponding to different zones, groups of zones, access points or groups of access points. In an embodiment, SSID's can be programmed to correspond to overlapping access points or zones. For example, a plurality of SSID's can be assigned to the same access point or zone. The Administrator setup page can also provide for temporary (or permanent) custom SSID's corresponding to a plurality of access points or zones. For example, a conference can be set up with with a personalized SSID corresponding to a set of access points or zones.

[0041] In an embodiment, the Administrator setup page can also allow an administrator to assign an amount of bandwidth to a particular access point, group of access points, zone, group of zones or SSID. For example, the Lobby may be provided less bandwidth than the Guest Rooms. Similarly, a conference with a custom SSID can be provided a set amount of Bandwidth for users of the custom SSID.

[0042] FIG. 5 illustrates a flow chart of a decision tree for determining when a login is required to obtain network access in an embodiment. At block 510, a subscriber's access point (labeled as Port-Location) has changed. The system moves to decision block 503 where the system determines whether or not the relogin after migration is enabled. If it is not, then the system allows users to migrate freely between access points at block 505. If the relogin after migration is enabled, then the system moves to decision block 507 where the system determines whether or not zones have been specified. If there are no zones specified then the system will require a relogin at each access point at block 509. If zones have been specified, then the system moves to decision block 511. At decision block 511, the system

determines whether the access point, or port in FIG. 5 is within the same zone as the previous access point used by the user. If the answer is no, then a relogin is required at block 513. If the access point is within the same zone, then the system moves to decision block 517. At decision block 517, the system determines whether relogin is required within a zone. If no, then no relogin is required at block 515. If yes, then the user is required to relogin at block 519.

[0043] In an embodiment, an administrator can separately define different access rights when moving between zones. For example, in an embodiment, anytime a user moves between zones they are required to login. This type of system is illustrated in FIG. 5. In an embodiment, an administrator can specify that users can move between certain zones without requiring re-authentication while requiring re-authentication when moving to other zones. This type of system is illustrated in FIG. 6.

[0044] FIG. 6 illustrates a flow chart showing when a login is required when moving between different zones in an embodiment. FIG. 6 illustrates four zones, lobby 601, business center 605, guest rooms 603, and meeting room A 607. As illustrated, when a user moves from guest rooms 603 to lobby 601, no relogin is required. When a user moves from lobby 601 to guest rooms 603, a relogin is required. When a user moves between the guest rooms 603 and the business center 605 no relogin is required. When a user moves from the guest rooms to the meeting room A, no relogin is required, but when a user moves from meeting room A to the guest rooms, a relogin is required. When a user moves from meeting room A 607 to the lobby 601, no relogin is required, but when a user moves from the lobby to meeting room A, a relogin is required. When a user moves between the meeting room A and the business center, a relogin is required. When a user moves from the business center 605 to the lobby 601, no relogin is required, but when a user moves from the lobby 601 to the business center 605, a relogin is required. Although FIG. 6 has been described with respect to certain named zones, it is to be understood that any number of zones, zone names, or zone locations can be used with the present system. Also, although described with respect to a relogin, any type of reauthentication can be used to move between zones.

[0045] In an embodiment, migration between zones can be further configured to use a "home" authentication or initial authentication location to track migration policy. This

allows a user, for example, to move from a first zone to a second zone and back to the first zone without a relogin in a system that generally requires a relogin to move from the second zone to the first zone. FIG. 7 illustrates an example timeline of two users moving between different locations in a network which uses a home authentication feature to track migration permission. As illustrated in FIG. 7, User A's 701 initial login is in the guest wireless zone at block 711. The network places into memory User A's initial authentication location and refers back to User A's initial authentication location when to determine migration access rights. User A 701 then moves to the lobby at block 713, then to the business center at block 715 and then back to the guest room at block 717 without relogin. However, when the user moves to meeting room A at block 719, a relogin is required. At this point, the home login can be changed to "meeting room A" or the home login can be both "guest wireless" and "meeting room A" providing permissions to both home authentication permission sets. User B's 751 initial login is the meeting room A at block 761. The user then moves to lobby at block 763 and then back to meeting room A at block 765 without requiring a relogin. However, when the user moves to the guest wireless zone at block 767, a relogin is required. Again, the home login is then altered to either "guest wireless" or both "guest wireless" and "meeting room A."

[0046] Conditional language used herein, such as, among others, "can," "could," "might," "may," "e.g.," and the like, unless specifically stated otherwise, or otherwise understood within the context as used, is generally intended to convey that certain embodiments include, while other embodiments do not include, certain features, elements and/or states. Thus, such conditional language is not generally intended to imply that features, elements and/or states are in any way required for one or more embodiments or that one or more embodiments necessarily include logic for deciding, with or without author input or prompting, whether these features, elements and/or states are included or are to be performed in any particular embodiment.

[0047] While certain embodiments of the inventions disclosed herein have been described, these embodiments have been presented by way of example only, and are not intended to limit the scope of the inventions disclosed herein. Indeed, the novel methods and systems described herein can be embodied in a variety of other forms; furthermore, various

omissions, substitutions and changes in the form of the methods and systems described herein can be made without departing from the spirit of the inventions disclosed herein. The claims and their equivalents are intended to cover such forms or modifications as would fall within the scope and spirit of certain of the inventions disclosed herein.

WHAT IS CLAIMED IS:

1. A method for determining whether to allow a network user communicating with a first access location within a privately controlled computer network including multiple access locations to migrate from one access location to another access location without re-authentication, the method comprising:

providing a plurality of network access locations configured to provide one or more user device's access to a privately controlled computer network;

defining migration permissions for migrating between individual network access locations in the plurality of network access locations, where the migration permissions establish migration rights between individual network access locations in the plurality of network access locations without requiring a user to re-login;

allowing a user device to migrate from communicating with a first network access location in the plurality of network access locations to a second network access location in the plurality of network access locations without requiring the user to re-login; and

requiring the user to re-login when migrating from the first network access location to a third network access location.

2. The method of Claim 1, wherein the network access location is a port.

3. The method of Claim 2, wherein the port is a VLAN port.

4. The method of Claim 1, wherein the first and second network access locations are comprised in a first zone of network access location and the third network access location is comprised in a second zone of network access locations.

5. The method of Claim 4, wherein the first zone comprises network access locations located in a first physical area and the second zone comprises network access locations located in a second physical area.

6. The method of Claim 4, further comprising assigning a first SSID to the first zone and a second SSID to the second zone.

7. The method of Claim 1, further comprising assigning a first SSID to the first and second network access locations and a second SSID to the third access location.

8. A system for providing computer network access in a secure computer network including a plurality of computer network access points, the system comprising:

one or more network management devices configured to provide network communications services for one or more network enabled devices; and

a plurality of network access points configured to provide communications portals for facilitating communications between the one or more network management devices and the one or more network enabled devices, the one or more network access points are controllable by the one or more network management devices to allow or deny communications via a second network access point of the plurality of network access points based on an authorization to use a first network access point of the plurality of network access points.

9. The system of Claim 8, wherein the network access points are organized into a plurality of zones, wherein each zone includes at least one network access point.

10. The system of Claim 9, wherein at least one SSID is assigned to at least one zone in the plurality of zones.

11. The system of Claim 10, wherein at least two SSID's are assigned to the at least one zone in the plurality of zones.

12. The system of Claim 9, wherein the one or more network management devices allow communications via the second network access point if the first access point is in the same zone and deny communications via the second network access point if the second network access point is in a different zone.

13. The system of Claim 9, wherein the one or more network management devices define the zone of the first network access point as a home zone and allow communications with other access points in the plurality of access points corresponding to a second zone if the home zone is defined to allow access to the second zone access points.

14. The method of Claim 8, wherein the network access point is a port.

15. A method of providing a user the ability to move between different locations of network access without requiring re-authentication comprising:

defining one or more zones, each zone including a plurality of network access locations;

allowing a network user to move from a first network access location in the plurality of network access locations to a second network access location in the plurality of network access locations without requiring re-authorization to access the second network access location, where the first network access location and the second network access location form part of a first zone in the one or more zones; and

requiring re-authentication from the user when moving from either the first or second network access locations to a third access location, where the third access location is not part of the first zone.

16. The method of Claim 15, wherein the network access location is a port.

17. The method of Claim 15, wherein re-authorization is required to access a network access location forming part of a second zone.

18. The method of Claim 15, wherein defining comprises assigning one or more network address locations to a zone.

19. The method of Claim 15, wherein re-authentication comprises using a login screen.

20. A system which provides access rights to a secure computer network based on a physical location of a user, the system comprising:

a network interface configured to communicate with one or more network enabled user devices and to communicate with other network devices, the network interface configured to provide communications between the one or more network enabled user devices and the other network devices;

a database configured with location dependant network access rights; and

a processor in communication with the network interface and the database, the processor configured to allow or deny network communications through the network interface based on a first location dependant authorization for a network enabled user devices at a first location to communicate through the network interface, the processor further configured to allow communications for the network enabled user device at a second location without re-authorization and require reauthorization for the network enabled user device at a third location.

21. The system of Claim 20, the location of the network enabled user device is determined based on a port accessed by the network enabled user device.

22. The system of Claim 21, wherein the location dependant network access rights are configured to provide access without re-authorization between ports that form part of a first zone, the first zone including one or more ports, and to require re-authorization when the network enabled user device migrates to a port in a second zone, the second zone including one or more ports.

23. The system of Claim 20, wherein authorization comprises one or more of a login, payment of fees, a request for access, or entry of a code.

24. The system of Claim 20, wherein authorization comprises the payment of a fee.

25. The system of Claim 20, wherein a first SSID is assigned to the first location.

26. The system of Claim 20, wherein a plurality of SSIDs are assigned to the first location.

27. The system of Claim 20, wherein a first SSID is assigned to the first and second locations and a second SSID is assigned to the third location.

28. The system of Claim 27, wherein a third SSID is assigned to the first, second and third locations, and wherein a second network enabled user device configured to access the third SSID is allowed to access the first, second and third locations without re-authorization.