

LANCOM™ Techpaper

Advanced Routing and Forwarding (ARF)

IP network virtualization

An ever increasing number of business applications such as telephony, remote maintenance and similar are using the advantages of IP networks.

With its Advanced Routing and Forwarding LANCOM Systems GmbH offers an elegant means of running all IP applications over a single router while at the same time keeping the various communications channels separate from each other.

In this process a dedicated IP network is established for each application or for different user groups. Data traffic between the networks and access to the Internet and to other remote networks is managed separately for each IP network by means of a virtual router. This process is also called **IP network virtualization**.

IP service convergence

Communications between companies and their customers, suppliers, employees and external service providers are increasingly being concentrated on one common technical platform: IP-based networks. IP networks are a standard that is available almost everywhere (even for users on the move using wireless networking and UMTS), sufficient bandwidth is available for all applications, and technologies such as VPN provide the necessary security to transfer even sensitive information over public networks such as the Internet.

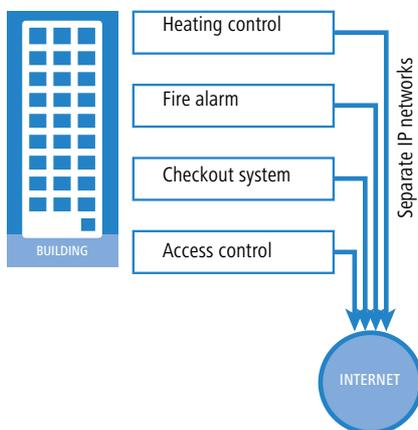
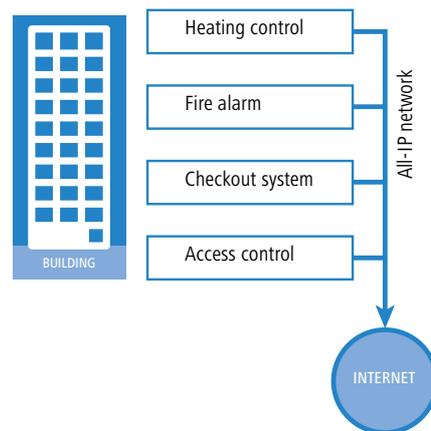
The widespread availability and acceptance, the cost benefits and the easy administration of IP networks mean that applications that hitherto had their own networks such as telephony are now using the IP network as a technical platform → VoIP (Voice over IP). Furthermore, new applications are also emerging in IP networks such as for example the exchange of information between management information systems (MIS), heating and air conditioning control or the update of spots on promotional terminals. Such networks in which all applications are implemented over just one network are also known as "all-IP networks".

However, the potential of all-IP networks has not yet been exploited to the full. Even when all security mechanisms are used to their full extent an external user is generally given access to a company's internal LAN (intranet) – something that in many cases is undesirable for reasons of security. Alternatively, a dedicated network is set up for each component with its own interfaces as in the case of for example machine controls with integrated modems, fire alarm systems with dedicated lines to the fire department, or separate routers for dial-in access. This second option leads to greater complexity and effort for IT departments due to the existence of parallel

networks with differing technologies—instead of the desired savings, the overall costs for communications and information exchange increase.

Dedicated IP network for each application

With Advanced Routing and Forwarding (ARF) LANCOM Systems provides all of the possibilities for the secure implementation of all-IP networks over a single, central router. The core of ARF is the ability to set up a separate IP context for each and every different application. Each IP context is configured as if it were a separate network e. g. with its own DHCP and DNS server and is shielded from all other networks. In this way several external users with differing requirements can be integrated into an organization's internal IP network without being granted access to the private intranet. Thus separate communications networks are no longer required for each application, and maintenance and configuration can be carried out at one central location.



Example applications

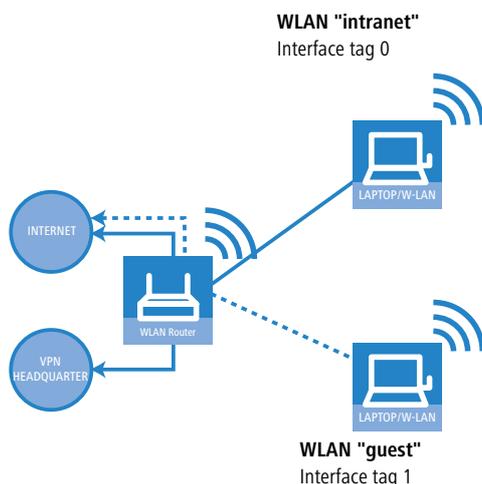
Advanced Routing and Forwarding comes into play when different groups of users share a common physical IP network. The following examples show possible applications that can be used alone or in conjunction with one another to set up an all-IP network.

- Guest access for WLAN clients
Nowadays guest access for mobile wireless clients is standard in most organizations. This enables visitors during a meeting to use their notebooks to dial into

LANCOM™ Techpaper

Advanced Routing and Forwarding (ARF)

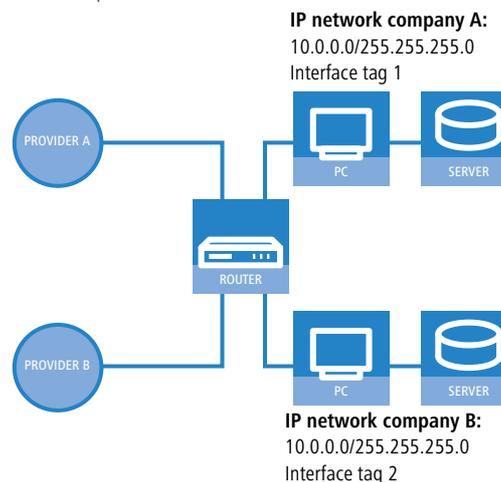
their own organization, for example via VPN, and to access the latest information there.



When using ARF, a separate IP network is set up for the guest wireless network in which a dedicated DHCP server distributes IP addresses which, for example, may be taken from a different address range than that used in the intranet. The IP network is given an interface tag which the router can use to differentiate the data traffic from that in the intranet.

- Shared WAN access
If several organizations share a building (e. g. branch offices of large companies), a separate Internet access need not be installed for each organization. The branch offices can use a central router that assumes the task of forwarding data appropriately. For each branch office a separate IP network is set up, each with a different interface tag. Both IP networks can even use the same IP address range if, for example, the IT department at headquarters requires special addresses. The data is identified by the router on the basis of the interface tag and thus can be handled using specific routing rules. For example the address range 10.0.0.0 at the savings bank branch can be routed to the head office of the savings bank via VPN while the same address range (10.0.0.0) at the insurance office branch can

be routed to the network of the insurance company's headquarters.



Alternatively the same technology allows each of these branch offices to make use of their own Internet providers. The routing table can allocate a special default route for each IP network to achieve this.

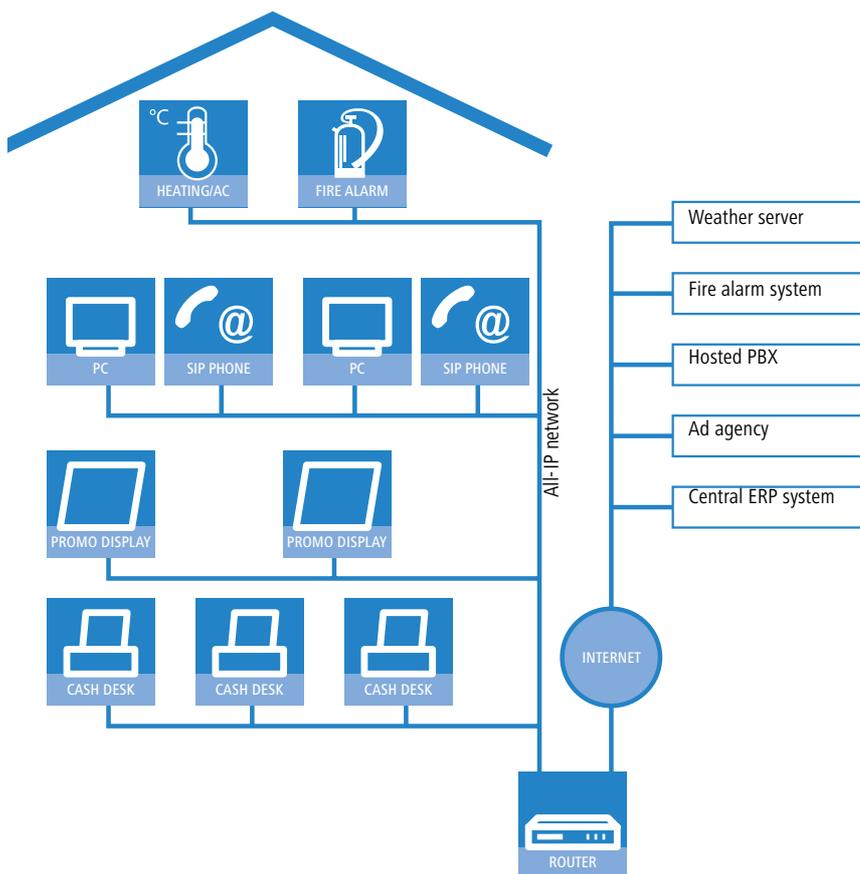
- Separating private and business IP networks in a home office
Many teleworkers are connected via a VPN to their company's central network in order to access the central mail system, databases or VoIP telephone systems. In the conventional version without ARF, the entire home office intranet with all its registered computers is linked to the company's central network. Using ARF, separate networks can be set up in the home office for business and private use ensuring that only the workstations intended for business use can communicate with the company via the VPN tunnel. The private computers obtain access to the Internet only. In the same way separate networks, such as in a school, can be set up for students and teachers with the pupils only having restricted access to the available resources.
- Sharing central resources
Thanks to ARF, different IP networks can be completely separated from each other - even when they share the same physical transmission medium. However, access from different IP networks is necessary in order to share central resources such as network printers or similar.

LANCOM™ Techpaper Advanced Routing and Forwarding (ARF)

The transfer of data between different networks is controlled by the firewall in the LANCOM Routers. Access to specific devices or services in a shared network can also be set up via the firewall in a similar manner.

- Integrating external service providers
In the applications shown so far the functionality of ARF has mainly been used to separate the users within the router itself on the basis of user group and to grant them the services and access to resources that they are permitted to use.

However, the possibilities of ARF also allow external resources or companies to be selectively integrated into a company's own infrastructure. Let's take a fully digitalized department store as a broad example.



- The store checkouts are networked and should report on the flow of goods several times a day to the ERP system at headquarters, which can then prepare for replenishment.
- The building's technical system obtains the latest weather forecasts from an Internet server and uses these to control the heating and air conditioning systems in advance.
- The video spots on the promotional displays are transferred from an external service provider and updated daily.
- VoIP telephones are used throughout the building and are connected to a telecommunications system located with an external service provider (hosted PBX).
- The alarm and security system is connected to the security company, which is automatically informed when an alarm or malfunction is triggered.

How does ARF work?

Advanced Routing and Forwarding consists of the following individual features:

- Several IP networks can be defined in the LANCOM Router.
- Individual IP networks are separated from one another.
- Different IP networks are routed separately.

Up to 64 IP networks in one router

The first feature depends on the hardware version. Depending on the model, the LANCOM Routers can manage up to 64 different IP networks and thus model complex scenarios. The IP address range used, the LANCOM Router's IP address and important functions such as DHCP and DNS server can be set up separately for each IP network.

Network name	IP address	Netmask	Network type	VLAN ID	Inte
INTRANET	0.0.0.0	255.255.255.0	Intranet	0	Any
DMZ	0.0.0.0	255.255.255.0	DMZ	0	Any
COMPANY	10.0.0.0	255.255.255.0	Intranet	0	Any
PUBLIC	10.1.0.0	255.255.255.0	Intranet	0	Any
PROMODISPLAY	192.168.0.0	255.255.255.0	Intranet	0	Any
VOIP	10.2.0.0	255.255.255.0	Intranet	0	Any

Separating networks

An essential condition for the secure operation of different IP networks in one device is the possibility to shield the data flows of the individual networks from one another. The networks are connected to the router via the

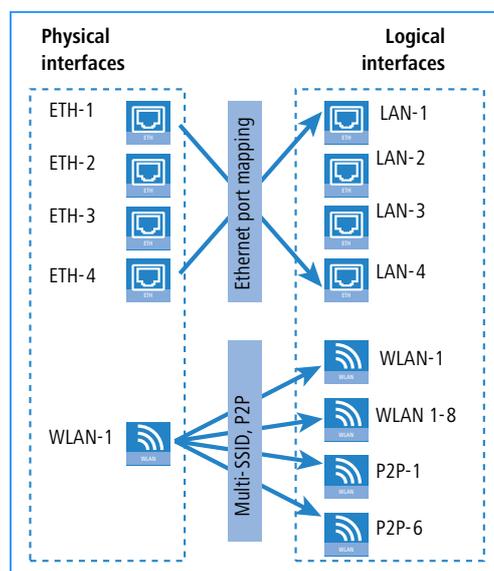
LANCOM™ Techpaper

Advanced Routing and Forwarding (ARF)

physical interfaces. Depending on the model, LANCOM Routers and LANCOM Wireless Routers provide one or several Ethernet ports and wireless modules to link local workstations and other network elements. However, these physical interfaces are not directly used for routing—the physical interfaces are bound to logical ones in order to provide the highest possible degree of flexibility.

Ethernet port mapping is used to perform this allocation for wired LAN connections: The desired utilization can be specifically configured for each Ethernet port, for example as a logical LAN interface (or with some models it is possible to configure the utilization as a WAN connection to link to a DSL modem).

In the case of wireless interfaces (WLAN modules), establishing point-to-point connections (P2P) and/or using multiple SSIDs means that multiple WLAN interfaces are assigned to each physical WLAN module: Up to eight wireless networks (multiple SSIDs) and up to six P2P connections per module, each of which appears to the router as a logical WLAN or P2P interface.



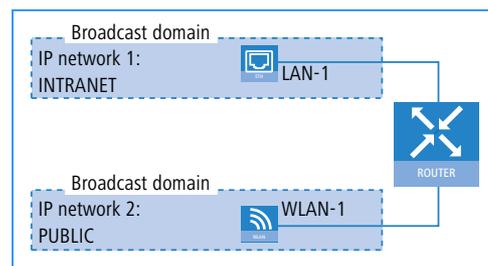
Each IP network can use one of the logical LAN, WLAN or P2P interfaces to access the physical interface behind it. The network is therefore in a separate broadcast domain and can only communicate with the router module of the LANCOM devices via this logical interface—**direct** data transmission to another network is not possible. A broadcast domain represents an area of a local network in which a broadcast message reaches **all** users. Broadcasts can also be transmitted across switches or bridges. Only when a router is used or when a local

network is split into VLANs (virtual LANs) is a broadcast domain restricted.

The decision about data transmission between the individual IP networks is thus transferred to the router in which the data streams from all IP networks converge. Routing between the different local IP networks is in principle allowed. Here's an example:

- The first IP network uses the address range 10.0.0.0 and is connected via the logical interface "LAN-1" to the physical interface "ETH-1".
- The second IP network uses the address range 192.168.0.0 and is connected via the logical interface "WLAN-1" to the physical interface "WLAN-1".

A DHCP server is activated for each network in the LANCOM. Although both networks are in separate broadcast domains, access to resources in the other network is made possible via the router.



A ping or a connection using an IP address is correctly resolved and forwarded. On the other hand, access to network devices using the Windows network environment is not possible as the NetBIOS broadcasts required for this do not leave the confines of the broadcast domain. Access to the Windows network environment can still be set up with a shared WINS server or a shared Active Directory structure.

The router's span of control can be easily tested by implementing a Deny-All rule in the firewall: This stops data traffic between all reachable networks via the router and a ping to another of those networks remains unanswered.

Controlled routing with interface tags

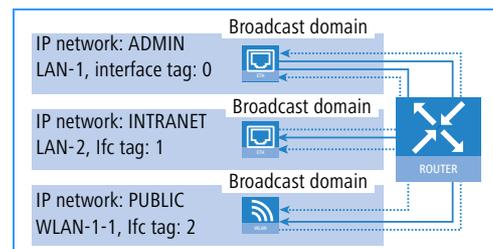
In addition to switching off all routing between IP networks it is also possible to select which IP network can access other specific areas via the router. If there is a large number of networks it may be necessary to configure a large number of firewall rules. To simplify the routing between logical interfaces, each IP network is given an interface tag. This tag provides a very elegant manner in which IP networks are interconnected via the router:

LANCOM™ Techpaper

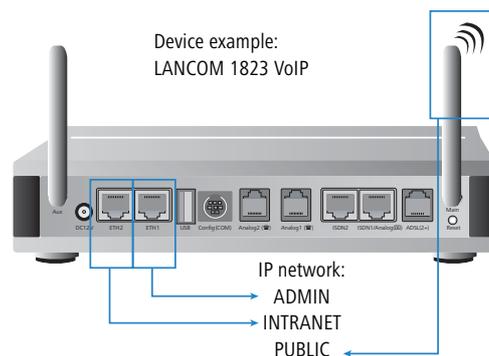
Advanced Routing and Forwarding (ARF)

- Network devices in an IP network can only access resources in networks with the same interface tag.
- An attempt to access networks with different interfaces tags is blocked in the router
- The interface tag "0" identifies the supervisor network: Devices in this network can access resources in all other networks that have a different tag.

i The interface tag controls the visibility of "intranet" type IP networks. In addition to intranets, networks can also be configured as a "DMZ" (demilitarized zone). The network type "DMZ" denotes an IP network whose resources can be accessed by users from all other IP networks regardless of the interface tags used.



For example, the system administrators' network is given the interface tag "0"—the administrators have access to all other networks. The networks for the intranet and the guest WLAN are given the interface tags "1" and "2" respectively—so remaining cut off without access to any of the other networks.



i As mentioned above, the firewall in the router is responsible for forwarding the packets of data. The firewall in the LANCOM is "stateful", meaning it can take the direction of the data connections into account. Therefore, access from the supervisor network with interface tag "0" to

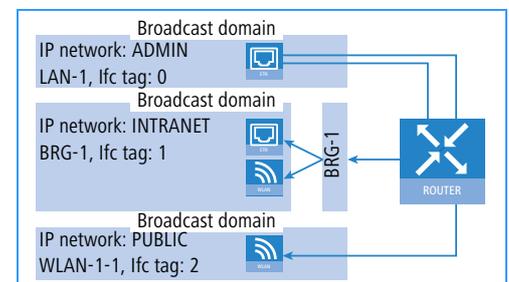
one of the other IP networks also opens the door to the flow of returning data. A computer in the guest network can therefore reply to a ping that was sent from a computer in the supervisor network.

Virtual interfaces

With some applications it is necessary to extend the explicit mapping of IP networks to logical interfaces. In a further step, logical interfaces can be mapped to "virtual" interfaces. Depending on the availability of logical interfaces, two scenarios are possible:

- Several logical interfaces are bundled to form one virtual interface: An IP network should not just connect computers from a wired LAN but also from a wireless LAN. In this case the logical interfaces required (e.g. a LAN and a WLAN for the intranet) are merged to form a so-called "bridge group" (BRG).

i Bridge groups are available in devices with a WLAN module in order to enable, for example, layer 2 WLAN networks (SSIDs) or VLANs to be bundled with dedicated Ethernet ports.



The bridge group defines its own broadcast domain, specifies which logical interfaces are assigned to it and acts for the router like a single virtual interface. In bridge mode, simple data transfer is possible between the connected logical interfaces of the bridge group—all other logical interfaces can only communicate with the bridge group via the router.

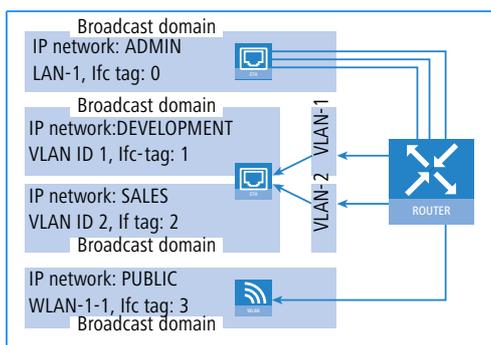
- A logical interface is used by several virtual interfaces: The reverse case occurs when the device does not provide enough logical interfaces to enable every IP network to be uniquely identified. In this situation several virtual LANs (VLANs) are defined that then use the same logical interface. For this, the IP network and additionally the logical interface are assigned with a VLAN ID. A VLAN ID is inserted into data packets whenever packets are sent from the IP network. If a packet with this VLAN ID is received

LANCOM™ Techpaper

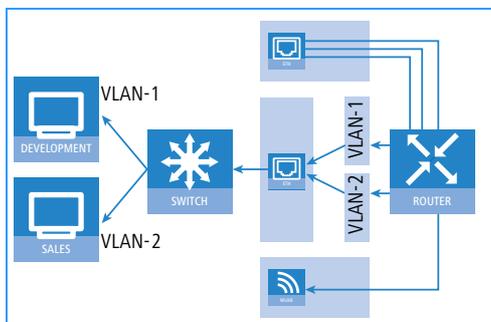
Advanced Routing and Forwarding (ARF)

over the logical interface, the packet can be assigned to the relevant IP network.

VLANs appear as separate virtual interfaces to the router—the data flows of the individual VLANs are however shielded from each others as each VLAN represents a separate broadcast domain.



It is thus possible for example to set up two networks for development and sales with different VLAN IDs on one logical LAN interface. The router takes care of the correct assignment and evaluation of the VLAN tags internally. Within the LAN, data packets are separated on the basis of the VLAN tags either in the network adapters or in an additional VLAN switch.



In this scenario too, interface tags govern the transmission of data between the VLANs.

The use of this flexible method of assignment means that, in addition to the logical interfaces, there are numerous VLANs and bridge groups available as virtual interfaces which can be used in any application to separate the network data traffic from that of other networks.

Virtual routers

Defining IP networks and separating data traffic (through the assignment of interfaces and bridge groups or VLAN IDs) ensures the parallel operation of several local networks on one central LANCOM Router. The IP router is responsible for the connection to other networks. The

routes specified in the routing table apply to all local networks connected to the device—in contrast to the DHCP settings, for example, which are configured for each IP network separately.

The implementation of a separate router for each network is also realized by using the interface tag. The interface tags are very closely related to the routing tags used in the LANCOM for "policy-based" routing. The routing tags can be inserted by the firewall into the data packets of certain services. For these data packets the router initially uses only those entries in the routing table that are marked with the corresponding routing tag.

The interface tags work in the same way for Advanced Routing and Forwarding. These tags control not just the visibility of IP networks among on another but also the use of the routing table: For each IP network only those entries are used with routing tags matching the interface tag of the IP network.

In this process the routing tag "0" is of special importance: Routes with this tag are valid for all networks regardless of the interface tag. The specific selection of routes from the routing table means that a virtual router is created for each IP network.

The following example illustrates the big advantage of the virtual router: Based on the source of a data packet, a firewall can generally allocate a routing tag that is then used in the IP router to choose the appropriate route. However, this process is not sufficient when the router manages several IP networks with the same address range: A tag can no longer be allocated unequivocally on the basis of the source address. However, using the interface tag it is still possible to allocate the remote node even when network devices from different IP networks with identical IP addresses wish to set up a connection. Virtual routing works on the evaluation of the interface tags alone; it is not necessary to configure additional firewall rules. It is therefore possible to allocate a separate provider connection for each local network using a tagged default route in the routing table.

IP address	Netmask	Routing tag	Active	Router	Distance	Mask
192.168.0.0	255.255.0.0	0	Yes	0.0.0.0	0	Off
172.16.0.0	255.240.0.0	0	Yes	0.0.0.0	0	Off
10.0.0.0	255.0.0.0	0	Yes	0.0.0.0	0	Off
224.0.0.0	224.0.0.0	0	Yes	0.0.0.0	0	Off
255.255.255.255	0.0.0.0	2	Yes	PROVIDER_2	0	Off
255.255.255.255	0.0.0.0	1	Yes	PROVIDER_1	0	Off

The firewall is only required when local networks with the same IP addresses contain servers that are accessible from the Internet. In this case the connections are set up from the outside to the internal network. Data packets

LANCOM™ Techpaper

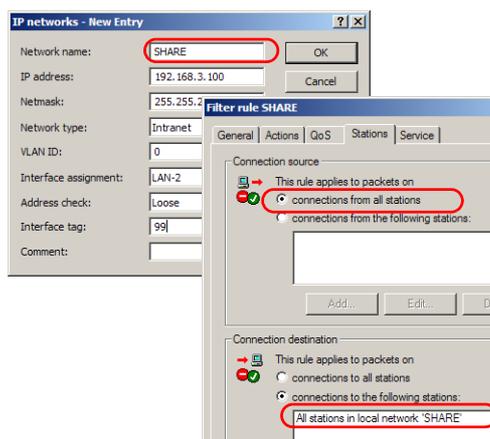
Advanced Routing and Forwarding (ARF)

arriving from the Internet at the router module do not have the interface tags that could be used for further processing. However, in this case the remote node from which the packets are received can be evaluated. Using a special firewall rule it is possible to allow connections from this remote node via the appropriate port (e. g. 80 for web servers) to the relevant network, with a corresponding port forwarding entry containing the explicit address of the web server.

Flexible transfer between IP networks

Advanced Routing and Forwarding allows completely separate networks to be implemented on one central router. However, some resources within the infrastructure may need to be made available to several or all networks, such as network printers not just for internal staff in the intranet but also for visitors in the public network. For this it is first necessary to set up a dedicated "SHARE" network for shared resources that is linked to the interfaces to which the shared resources connect. This network is also configured as an "intranet" with a unique interface tag (e. g. "99"). The network is therefore initially shielded from all other networks.

With a suitable rule in the firewall it is possible to set up access to the common SHARE network from all other network stations. This firewall rule includes the interface tag of the SHARE network as routing tag. All data packets corresponding to this firewall rule are thus given the tag "99" and can in this way be assigned to the SHARE IP network. If necessary, it is also possible to specify in the firewall rule those services which may be used in the SHARE network.



Summary

Advanced Routing and Forwarding in LANCOM Routers gives you the possibility of defining several networks in a single central device and of shielding the data flows in those networks from each other by allocating Ethernet and WLAN ports or assigning bridge groups and VLAN IDs. The possibility for local networks to communicate with one another is controlled by the router and by special interface tags.

Moreover, using interfaces tags you can also set up a dedicated virtual router that establishes the connection to the Internet or to other external remote nodes. It is thus possible to set up, for example, a VPN tunnel to a partner organization that is accessible only from specific individual networks.

The ARF routers can use these functions to create all-IP networks in which different IP-based applications can share a common infrastructure but yet remain separate from one another. Locally, several "intranets" or "guest" networks can be operated in parallel and external partners can be granted access via the Internet to parts of the local infrastructure.

 Please visit www.lancom.eu/support for concrete sample configurations and specimen scripts and search the LANCOM KnowledgeBase with the argument "ARF".