

Advanced Routing and Forwarding (ARF)

With the growing complexity of modern IP networks, the demands on the underlying infrastructure are increasing: Applications such as telephony, remote maintenance, guest access or security services must be set up and operated in parallel in a shared infrastructure while at the same time remaining securely separated from one another.

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

In this process, a dedicated IP network is established for each application or for the 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

Companies are communicating with customers, suppliers, employees, and external service providers on a common IP infrastructure.

The potential of these networks has often not been exploited to the full. Even when all security mechanisms are used to their full extent, external users are often given access to a company's internal LAN (intranet)—something that is often undesirable for reasons of security. Alternatively, each component can be set up with a separate network for its own interfaces. 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 actually increase.

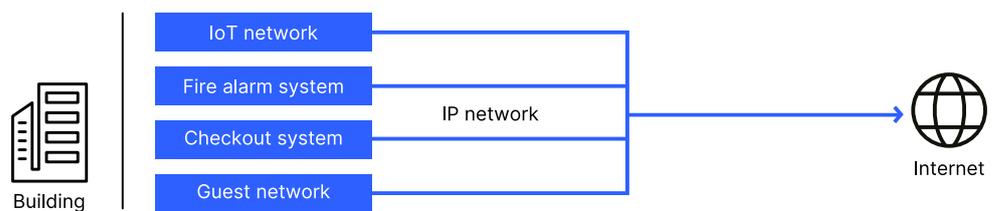


Figure 1:
Classic IP-based network without
application separation

Dedicated IP network for each application

With Advanced Routing and Forwarding (ARF) LANCOM Systems provides a wide range of options for the secure implementation of IP-based 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 it is isolated 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. Separate communications networks are no longer required for each application, and maintenance and configuration can be carried out at one central location.

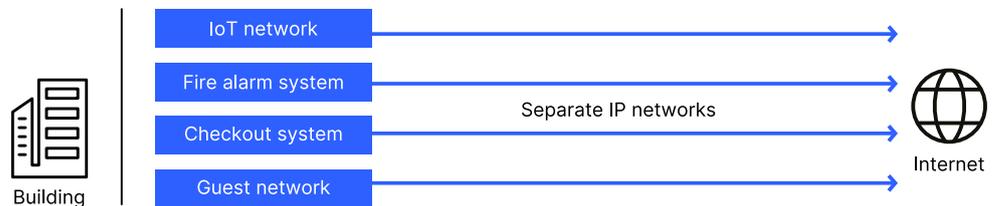


Figure 2:
IP-based network with
applications separated by ARF

Example applications

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

Guest access for Wi-Fi clients

Nowadays it is standard in most organizations for mobile wireless clients to have guest access. This enables visitors during a meeting to use their notebooks or smartphones to dial into their own organization, for example via VPN, and to access the latest information there.

ARF supports a separate IP network for the guest wireless network, where a dedicated DHCP server assigns IP addresses that can be from a different address range than that used for the intranet. The IP network is given an interface tag, which the router uses to distinguish this data traffic from that in the intranet.

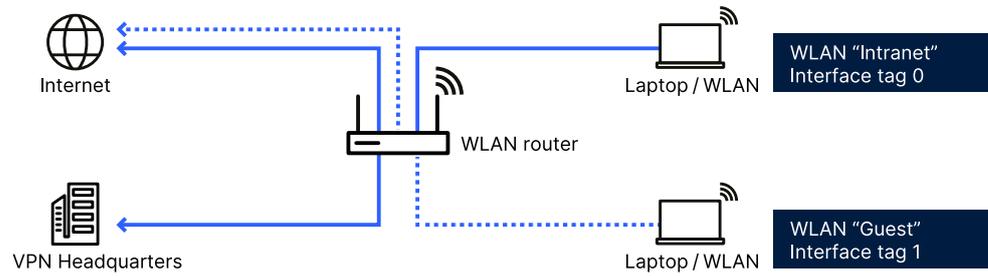


Figure 3:
Guest access for Wi-Fi clients

Shared WAN access

If several organizations share a building (e.g. branch offices of large companies), there is no need to install a separate Internet access for each organization. The branch offices can use a central router that handles the task of forwarding data. A separate IP network is set up for each branch office, with each network having a different interface tag. Both IP networks can even use the same IP address range if, for example, the IT department at the headquarters requires special addresses. The router uses the interface tags to identify the data, which can then be handled with dedicated routing rules. For example the address range 10.0.0.0 at the bank branch can be routed to the bank's head office 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 use their own Internet providers. The routing table can achieve this by providing a special default route for each IP network.

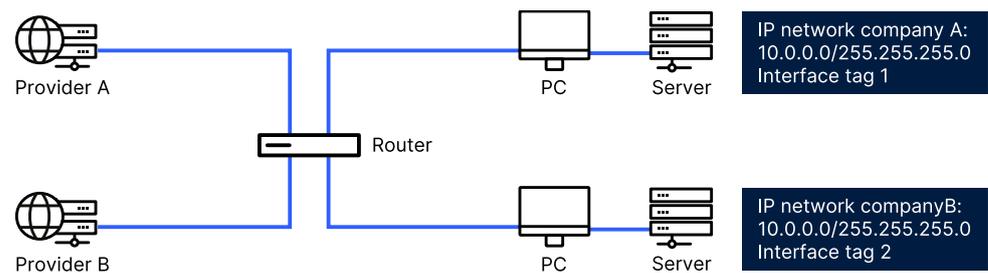


Figure 4:
Shared WAN access

Separating private and business IP networks in the home office

Many teleworkers are connected by VPN to their company's central network so that they can access the central mail system, databases or VoIP telephone systems. In the conventional scenario without ARF, the whole of the intranet at the home office, and all of the computers in it, are linked to the company's central network.

ARF allows separate networks for business and private use to be set up in the home office, which ensures that only those workstations intended for business use are able to communicate with the company via the VPN tunnel. The private computers obtain access to the Internet only. In the same way, networks in a school can also be separated for students and teachers, whereby the students have only limited access to the available resources.

Sharing central resources

Thanks to ARF, different IP networks can be completely separated from one another—even though they share the same physical transmission medium. However, access from different IP networks is required if central resources such as network printers are to be shared, for example. 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 access to the services and resources that they are permitted to use. However, ARF also allows the selective integration of external resources or other companies into a company's own infrastructure. Let's take a fully digitalized department store as a broad example.

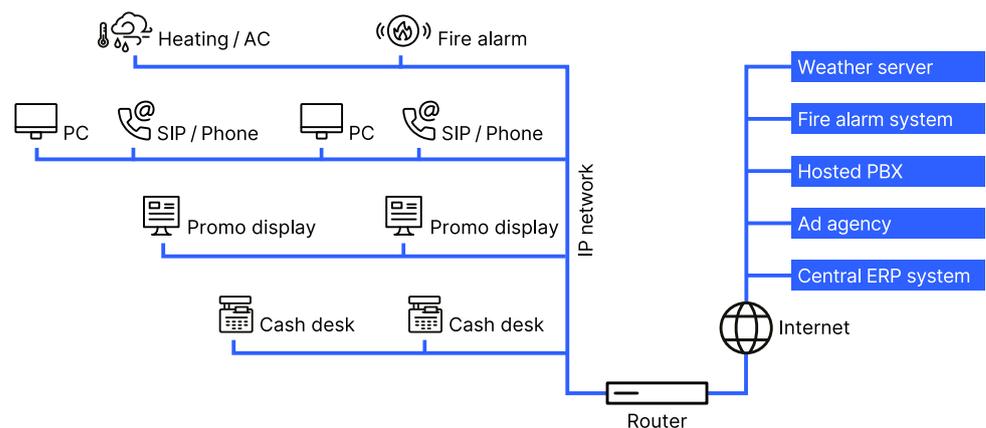


Figure 5:
Example of a digitalized
department store

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 hosted by an external service provider.
- The alarm and security system are connected to the security company, which is automatically informed when an alarm or malfunction is triggered.

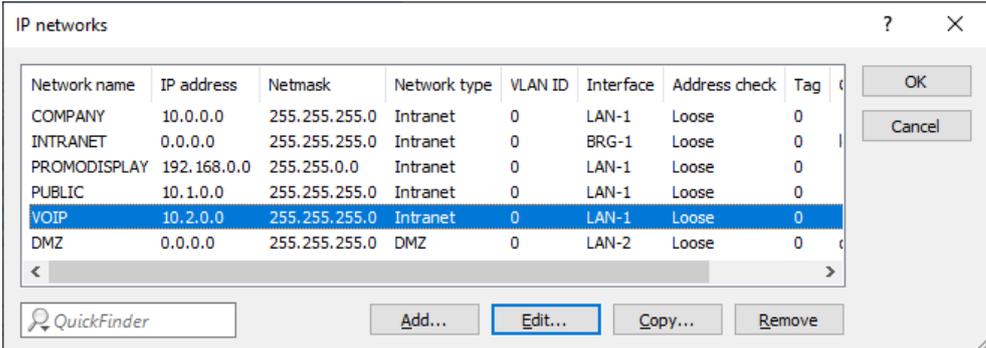
How does ARF work?

Advanced Routing and Forwarding enables the following:

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

Up to 256 IP networks in one router

The first feature depends on the hardware version. Depending on the model, LANCOM routers can manage up to 256 different IP networks and are thus able to model complex scenarios. The IP address range used, the IP address of the LANCOM router 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	Interface	Address check	Tag
COMPANY	10.0.0.0	255.255.255.0	Intranet	0	LAN-1	Loose	0
INTRANET	0.0.0.0	255.255.255.0	Intranet	0	BRG-1	Loose	0
PROMODISPLAY	192.168.0.0	255.255.0.0	Intranet	0	LAN-1	Loose	0
PUBLIC	10.1.0.0	255.255.255.0	Intranet	0	LAN-1	Loose	0
VOIP	10.2.0.0	255.255.255.0	Intranet	0	LAN-1	Loose	0
DMZ	0.0.0.0	255.255.255.0	DMZ	0	LAN-2	Loose	0

Figure 6:
IP networks configuration

Separating networks

An essential condition for the secure operation of different IP networks on 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 physical interfaces. LANCOM routers and LANCOM WLAN 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 the wireless network interfaces (WLAN modules), the establishment of point-to-point connections (P2P) and/or the use of Multi-SSID can mean that multiple WLAN interfaces exist on each physical WLAN module, each of which appears to the router as a logical WLAN or P2P interface.

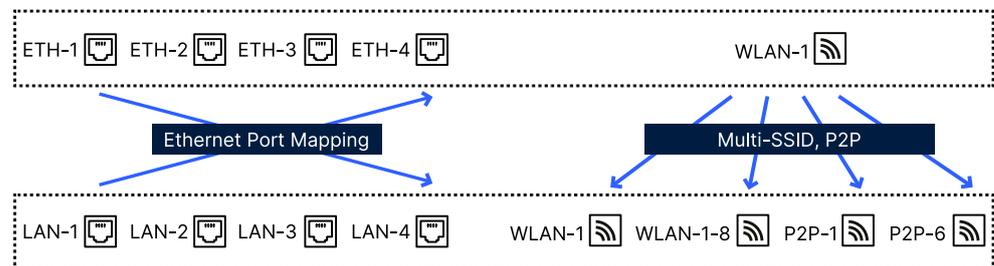


Figure 7:
Logically separated IP networks

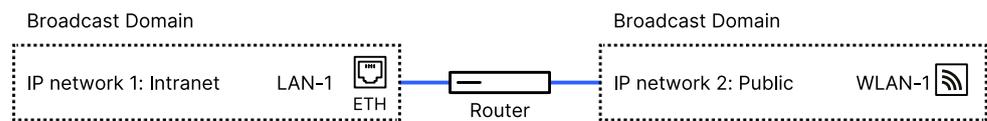
Each IP network can use one of the logical LAN, WLAN or P2P interfaces to access the physical interface behind it. The network is therefore in a separate broadcast domain and the logical interface only allows communication with the router module in the LANCOM devices—direct data transmission to other networks 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 where the data streams from all IP networks converge. Routing between the different local IP networks is in principle possible. 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 possible via the router.

Figure 8:
Limitation of broadcast domains
by routers



A ping or a connection using an IP address is resolved correctly and forwarded.

The router’s span of control is easily tested by implementing a Deny-All rule in the firewall: This stops data traffic between all reachable networks on the router, and a ping to another of those networks will go 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:

- 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 different tags.



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 with resources that can be accessed by users from all other IP networks—regardless of the interface tags used.

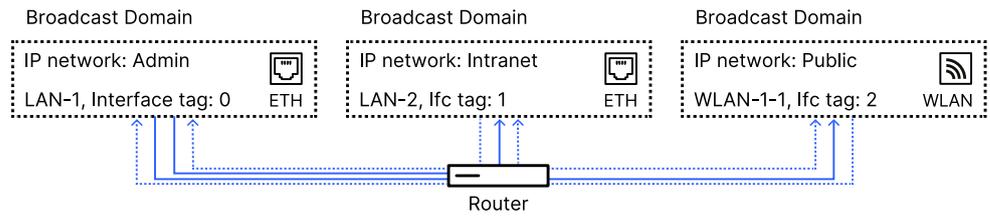


Figure 9:
An example of controlled routing with interface tags

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 isolated and without access to the other networks.

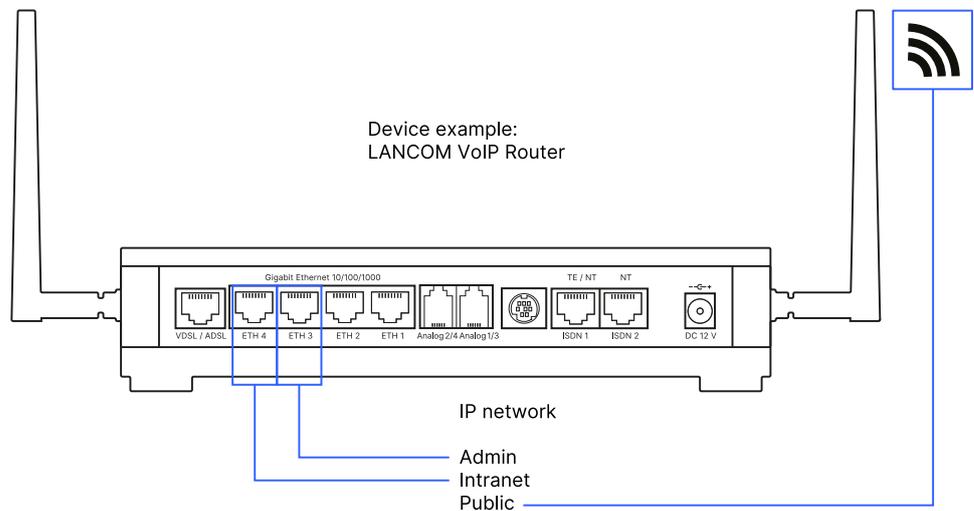


Figure 10:
Device example:
LANCOM VoIP router



As mentioned above, the firewall in the router is responsible for forwarding the packets of data. The firewall in the LANCOM router is "stateful", meaning that it is aware of the direction of the data connections. 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 the 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 only connect the computers on a wired LAN, but also those on a wireless

LAN. In this case the required logical interfaces (e.g. a LAN and a WLAN for the intranet) are merged to form a so-called “bridge group” (BRG).



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.

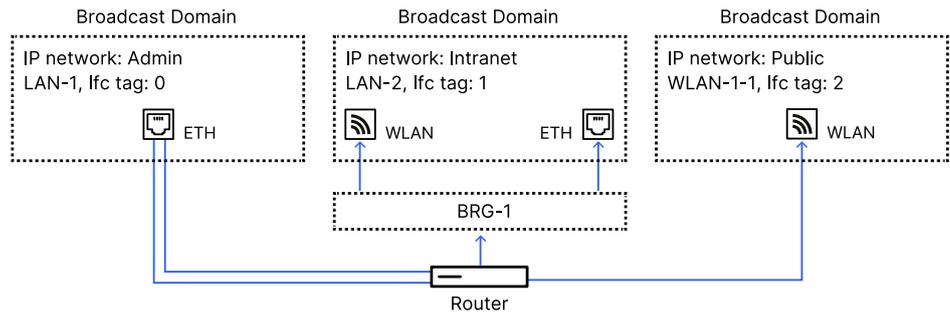


Figure 11:
Collecting physical interfaces into
bridge groups

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 bridge group’s interconnected logical interfaces—all other logical interfaces can only communicate with the bridge group through 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 each 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 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 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 one another, as each VLAN represents a separate broadcast domain.

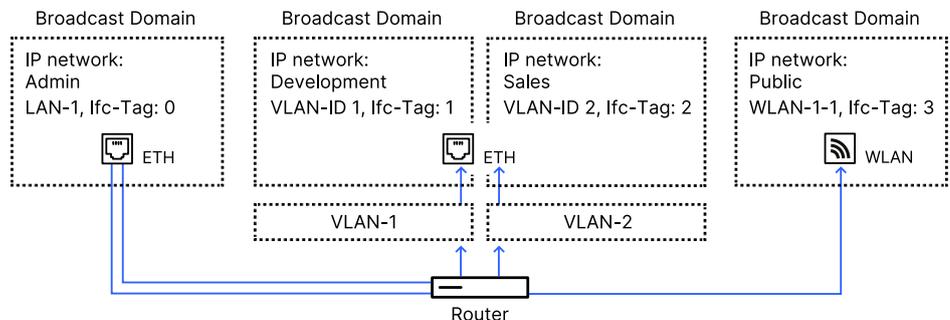


Figure 12:
Logical separation by VLAN

It is thus possible, for example, to set up two networks (e.g. for the Development and Sales departments) with different VLAN IDs on a single logical LAN interface. The router takes care of the correct assignment and processing of the VLAN tags internally. In the LAN, the data packets are separated using the VLAN tags either in the network cards of the workstations or in an upstream VLAN switch.

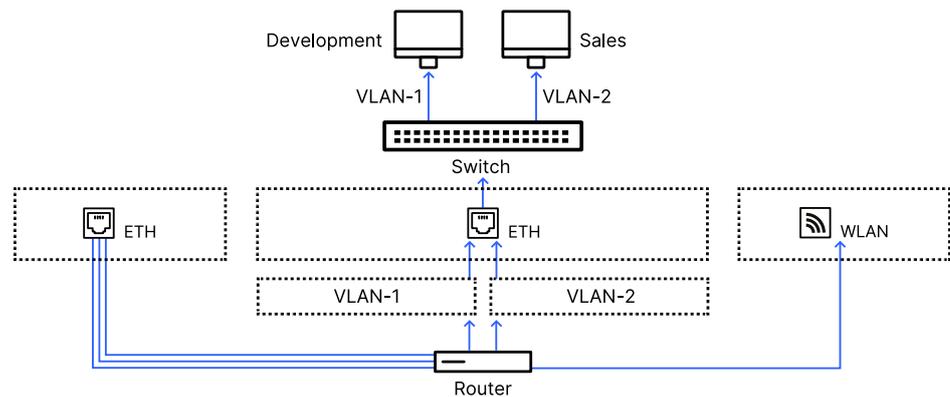


Figure 13:
Logical separation by VLAN
in the switch

In this scenario too, interface tags steer 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 for use by any application to keep network data traffic separate from that on other networks.

Virtual routers

Defining IP networks and separating data traffic (through the assignment of interfaces and bridge groups or VLAN IDs) ensures that several local networks can be operated in parallel on a single central LANCOM router. Connections between the networks are controlled by the IP router. Routes in the routing table apply to every local network connected to the device—in contrast to the DHCP settings, for example, which are configured for each IP network separately.

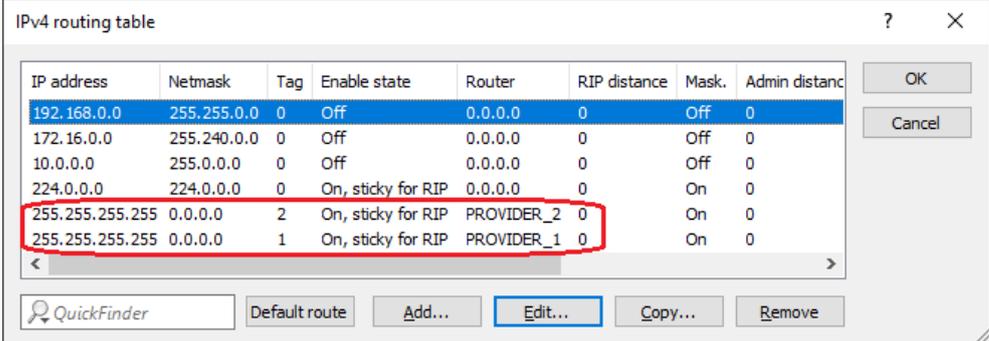
The interface tag is also used to implement a separate router for each network. Interface tags are very closely related to the routing tags used in the LANCOM router for “policy-based” routing. The firewall can insert routing tags into the data packets of certain services. For these data packets, the 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. As well as controlling the extent to which IP networks can “see” one another, tags simultaneously

control the way the routing table is used: Each IP network initially uses only those entries with routing tags that match the interface tag of the IP network.

In this process the routing tag "0" is of special significance: Routes with this tag are valid for all networks, regardless of the interface tag. This specific selection of routes from the routing table creates a separate virtual router for each IP network.

The following example illustrates the big advantage of the virtual router: Based on the data-packet source, a firewall usually assigns a routing tag that the IP router uses to set the correct route. However, this method is not sufficient if the router manages a number of IP networks with the same address range: Tag assignment based on the source address is no longer unequivocal. Nevertheless, 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 attempt 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. For each local network, a separate provider connection can be selected by using a tagged default route in the routing table.



IP address	Netmask	Tag	Enable state	Router	RIP distance	Mask.	Admin distance
192.168.0.0	255.255.0.0	0	Off	0.0.0.0	0	Off	0
172.16.0.0	255.240.0.0	0	Off	0.0.0.0	0	Off	0
10.0.0.0	255.0.0.0	0	Off	0.0.0.0	0	Off	0
224.0.0.0	224.0.0.0	0	On, sticky for RIP	0.0.0.0	0	On	0
255.255.255.255	0.0.0.0	2	On, sticky for RIP	PROVIDER_2	0	On	0
255.255.255.255	0.0.0.0	1	On, sticky for RIP	PROVIDER_1	0	On	0

Figure 14:
An example of IPv4 routing by
interface tags

The firewall is only necessary 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 arriving from the Internet at the router module do not contain interface tags for further processing. However, in this case the remote source where the packets are received from can be evaluated. A dedicated firewall rule can allow connections between this remote site and a particular port (e.g. 80 for web servers) to pass into the relevant network. A corresponding port-forwarding entry contains the explicit address of the web server.

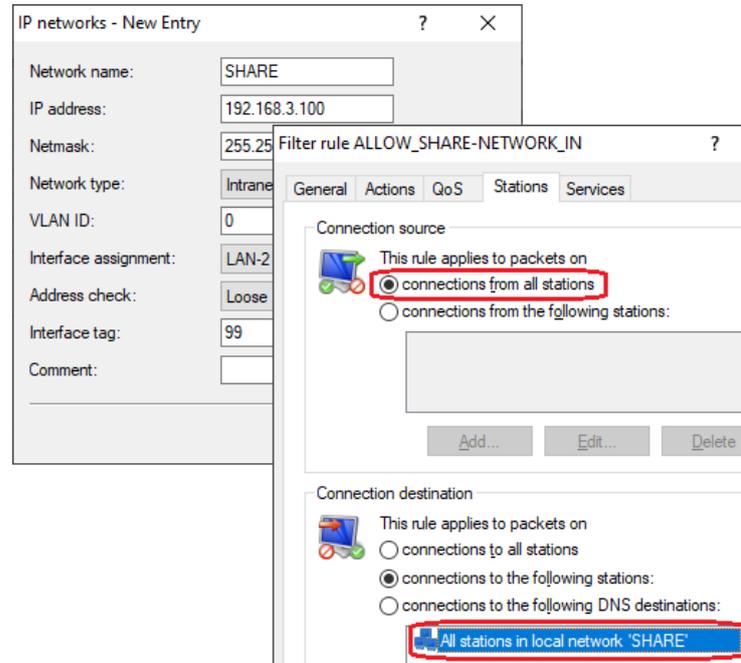


Figure 15:
Example of a firewall rule for
external connections

Flexible transfer between IP networks

Advanced Routing and Forwarding allows completely separate networks to be implemented on a single 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. This is linked with the interfaces that the shared resources connect to. 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.

LANCOM Management Cloud (LMC)

The LANCOM Management Cloud allows the management of complete networks with the use of software-defined networking technologies (SDN). SD-WAN automatically creates secure VPN connections between sites, including network virtualization and backups across the wide-area network (WAN): A few mouse clicks is all it takes to enable the VPN function and select the required VLANs for each site. The tunnel endpoints do not need to be configured individually. A VPN tunnel is required by each multi-site network

This is where Advanced Routing and Forwarding (ARF), which provides up to 256 IP contexts in conjunction with the LMC, is an elegant way to route all IP applications through one central router and keep the different communication channels securely separated.

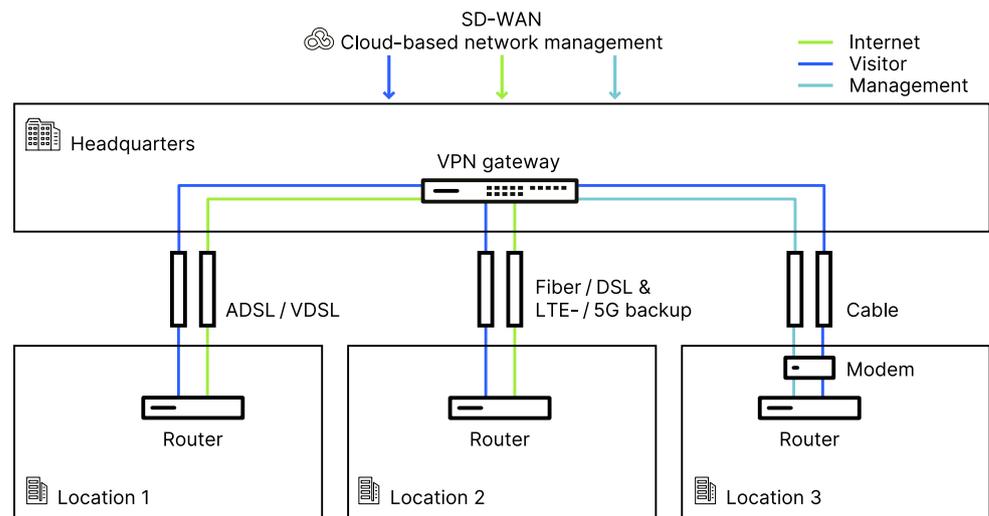


Figure 16:
SD-WAN uses ARF to logically separate communication channels

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 one another by allocating Ethernet and WLAN ports or assigning bridge groups and VLAN IDs.

Communications between local networks are 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.



Concrete examples of configurations and scripts are available in the LANCOM Knowledge Base by searching for the keyword "ARF".

www.lancom-systems.com/knowledgebase