Title

Security in Infinet Wireless Devices

Successfully pass the free certification exam at IW Academy and become an Infinet Certified Engineer.

To the certification exam

Table of contents

Introduction

The information technology evolution has changed the human life in all spheres, making information one of the most valuable resources. Same as other resources, information is valuable for its owner and can cause disputes and conflicts. That's why, the information security should be taken seriously into account. The information systems development and the large amounts of data accumulation require an integrated approach in ensuring the security of the technical systems.

This document describes the information security methods used in networks comprised of Infinet Wireless devices. Each wireless device family has its own capabilities of application security tools, so at the end of a document's section you will find links to the technical documentation of each described tool.

Terminology

- **Information** - knowledge about the world and the processes in it, perceived by a person or a special device.
- **Information Security (IS)** - the security of the information and of the infrastructure components which helps to ensure information confidentiality and integrity.
- **Technical company policy** - a set of technical solutions necessary to be used by the company's technical systems. The technical policy includes requirements for installation, operation and configuration of the devices. It is necessary to carry out periodical updates of the document and check its proper implementation.
- **Threat** - potential violation of the information security.
- **Attack** - attempt to realize a threat. An attack can be either malicious or not.
- **Attacker** - a person or group of people making an attack.
- **Echelon** - a subject for attack prevention, implemented as a part of an information security policy.
- **Risk** - the likelihood of a specific threat.
- **Responsibility area** - a network segment which has a certain subject responsible for its effective operation. A subject can be either a specific person or an organization.
- **Internal network segment** - a network segment that is in the responsibility area of our organization.
- **External network segment** - a network segment that is under the responsibility of a third-party organization or client. Since the external network segment is managed by a third-party organization, the crossing of the internal and the external network segments is a source of threats.

Information Characteristics

Information security measures should be applied in accordance with the company's IS policy. The IS policy should take into account the following information characteristics:

- **Accessibility** - the ability to access information in an acceptable time.
- **Integrity** - relevance and consistency of the information.
- **Confidentiality** - the impossibility of obtaining unauthorized access to information.

An information security policy should include measures to ensure each of the basic information characteristics. If the described information characteristics aren't respected, it may lead to financial, reputation and other loses. Remember that the IS policy implementation is an endless process that requires periodic review of the measures and of their implementation.

The IS organization should be multilevel and not only realized with technical solutions. In addition to technical measures, legislative, administrative and procedural measures should be provided.

Scenarios for Infinet equipment

The measures to ensure the IS are determined not only by the Infinet device family, but also by the scenario of their use (Figure 1a-d). Let's look at several scenarios in which wireless devices connect network segments belonging to different responsibility areas, each area being characterized by a certain set of threats:

- joining of internal network segments;
- connection of internal and external network segments;
- internal network segments connected with the Internet.

The security measures should correspond to existing risks, the IS architecture should not be redundant. For example, filtering of external connections should be performed at the interface on border with a third-party telecom operator, not on all the intermediate nodes of the network.

The requirements for physical safety and security in the radio link are the same for all the scenarios below and are described in detail in the relevant sections. In order to configure the devices, let's specify the following general requirements for information security:

- the management of the external devices should be limited by whitelists;
- service network protocols should not leave the internal network segment;
- at the border of responsibility areas, an internal segment should be protected from malicious traffic.

Joining of the internal network segments

The simplest scenario is joining two network segments located in the same responsibility zone (Figure 1a). The devices are used as a bridge using a simple connector in the LAN structure, therefore, the main information security tools are located at the boundaries of the left and right segments.

Figure 1a - Radio link joining two internal network segments

Connection of internal and external network segments

In the scenario of connecting two networks located in different responsibility areas, the information security measures are implemented on a radio device located at the border of the two segments. A special example of the external network segment is the client's network, which is provided with a data transmission service. In such scenarios, both inbound and outbound traffic should be filtered.

Figure 1b - Radio link connecting internal and external network segments

Figure 1c - Radio link connecting internal and external network segments

Internal network segments connected with the Internet

The scenario where a wireless device is located at the border of the internal segment and the Internet is a special case of the previous scenario's external network. The difference is in a low security on the device from the side of the Internet connection, that causes a large number of risks.

Figure 1d - Radio link connecting internal network segments and the Internet

Information security measures in various scenarios

The IS realization is achieved by the implementation of the measures described in the sections and in the subsections of the IS:

IS section	IS subsection	Application
Physical security	All	ALL SCENARIOS
Radio Security	All	ALL SCENARIOS
	Authentication	ALL SCENARIOS

Device management	Access method	LAN - EXTERNAL LAN LAN - WAN
	Management interface	ALL SCENARIOS
	Firewall	LAN - EXTERNAL LAN LAN - WAN
	Access recovery	ALL SCENARIOS
Data transmission	General recommendations	ALL SCENARIOS
	Data transmission settings	ALL SCENARIOS
	Network protocol settings	ALL SCENARIOS
Infrastructure	Monitoring	ALL SCENARIOS
	History storage	ALL SCENARIOS
	Technical Accounting	ALL SCENARIOS

Physical security

The physical layer is the foundation of the information security, so the devices' physical security has a priority within the company's technical policy. Physical security should be comprehensive and include several components:

- site selection for equipment installation;
- organization of auxiliary facility infrastructure;
- equipment installation;
- facility operation.

The communication node (including wireless devices) consists of three main elements (Figure 2):

- **High-rise part**: the location of wireless devices, for example, the roof of a building, a mast, a telecommunication tower.
- **Cable route**: cables connecting the high-rise part and the equipment located indoor.
- **Building**: equipment located indoor and points of connection to the infrastructure. The infrastructure may include data channels, power, climate systems, etc. The equipment should be placed in a rack or in a telecommunication enclosure, which can be placed in a dedicated room or can be combined with the high-rise part of the object.

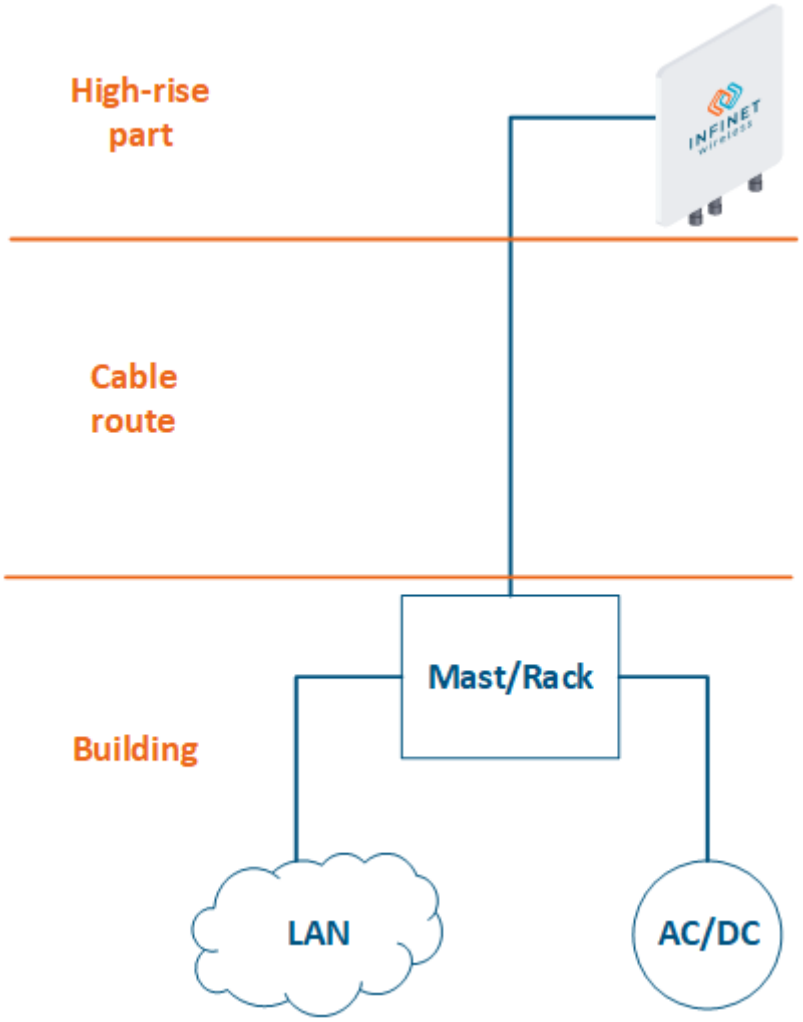

Figure 2 - Communication node block diagram

Site selection for the equipment installation

The site for the equipment installation must meet the requirements of the company's technical policy and allow future network scalability. The following aspects should be taken into account when choosing a site:

- **Access to the facility** is an important factor affecting the communication recovery time and the equipment maintenance time. Access to the facility should be limited in time and for white lists of employees. Access lists must be up to date. If access lists are not up to date, it can be used, for example, by a dismissed employee whose name was not promptly excluded from the lists. Pay attention on the guards and locks in the places where equipment is located in order to prevent unauthorized access.
- **A dedicated room.** It is recommended to place data transmission equipment and points of connection to the infrastructure in a dedicated room, isolated from external factors. For example, it can be a room with a separate entrance and access for the company employees only or a machine room where the third-party company equipment is located.
- **Cable route.** The site must meet the requirements for the cable route installation and for access during the operational phase. General requirements adherence for cabling is an important factor in reducing the risks associated with link accessibility, which can be caused by cable damage or connection errors.
- **Power.** The site must have a connection point with a stable power supply network. In accordance with the company technical policy, a backup line of electric power supply or an uninterrupted power supply system can be organized. Power supplies must be independent, i.e. there should be no single point of failure. For backup power supply systems, it is recommended to implement automatic switching schemes between sources, which will avoid communication interruption in case of the main power supply source failure.
- **Grounding.** Proper grounding can significantly reduce the likelihood of the wireless device's failure in case of electromagnetic noises or lightning strikes.
- **Climate systems.** The reliable network equipment operation depends on the external conditions: the device is guaranteed to function in the specified temperature range, pressure and humidity. The environment influence is random, therefore, in order to maintain a stable operation, the specified climatic conditions must be created artificially, it is recommended to install an air conditioner and a heater with the possibility of automatic on / off. The climate systems in the high-rise part are impossible, therefore, for reliable operation in harsh conditions, the devices of the InfiLINK 2x2 / InfiMAN 2x2 families with an extended temperature range can be used. Such devices are equipped with a built-in heater, which turns on when the ambient temperature drops below a set threshold.

- **Links.** The network accessibility can be increased by installing backup links. The links must be independent, i.e. the should be no single points of failure, for example, a wired communication channel can be the main one, and wireless can be the backup one. The realization of fault-tolerant schemes for automatic link redundancy and aggregation using Infinet devices are described in the Link aggregation, balancing and redundancy article. Scenarios including mobile objects require a different reservation scheme, described in the Connectivity with mobile objects article.

Organization of auxiliary facility infrastructure

An important factor in site choosing is the ability to install auxiliary infrastructure elements, which will increase the availability of the communication system. Video surveillance and alarm systems are examples of auxiliary infrastructure. An alarm allows to quickly detect an unauthorized access to the object and a video surveillance system will be useful in investigating incidents.

Equipment installation

The installation work on site should be guided by the general requirements and by the company's technical policy. Improperly executed, the installation can cause a violation of the entire network facility availability, the restoration of which may require a large time and financial resources.

In order to ensure the physical security, perform the following settings for the wireless device:

- turn off the indicator lights on the device, it will increase its stealth;
- the unused ports of the wireless devices can be used by an attacker to gain access to the network, therefore, in order to eliminate the possibility of unauthorized connections, it is recommended to disable the unused network interfaces;
- the devices based on the H11 hardware platform support the PoE-out function on eth1. An attacker can use it to power third-party equipment. If the PoE-out function is not used, make sure it is disabled.

Facility operation

The installation quality control is carried out in the phase of the acceptance into service of the device. The acceptance procedure should be performed in accordance with the company's technical policy.

Ensuring the information security is a continuous process that requires monitoring and response to identified and emerging threats, therefore, it is necessary to carry out preventive maintenance for the communication facilities. Depending on the requirements established by the company and the specifics of the network node, the list of preventive measures may vary. A common set of regular jobs includes:

- facility inspection to make a list of deviations from the technical policy requirements;
- cleaning on site;
- periodic testing of the backup systems: for links - scheduled work with the main channel turned off, for power systems - scheduled work with the main source turned off (additionally, uninterruptible power supplies and battery capacity testing).

Physical security implementation for device families

Physical security measures

Event / Interface	InfiLINK 2x2 / InfiMAN 2x2		InfiLINK Evolution / InfiMAN Evolution		InfiLINK XG / InfiLINK XG 1000		Quanta 5 / Quanta 6	Quanta 70
	Web	CLI	Web	CLI	Web	CLI	Web	Web
Mounting devices	InfiNet Wireless R5000 installation		Installation		Installation Procedure		Installation	Installation
LED indication management	-	General Commands	-	General Commands	-	General Commands	-	-
Interface Status management	Network Settings	Ifconfig command	Network Settings	Ifconfig command	Switch	Ifconfig command	Switch Settings	Switch Settings
PoE-out management	Network Settings	Ifconfig command	Network Settings	Ifconfig command	-	-	-	-
Heater control	-	Other commands	-	-	-	-	-	-

Radio security

Wireless data transmission is performed in a shared environment, which brings a lot of possibilities for the attackers. The security measures described below should be applied in a comprehensive manner, since measures protecting from one threat may not be effective against another.

Frequency configuration

The frequency resource is limited, so the frequency distribution between wireless systems should be carefully considered. Third-party wireless systems operating on the same or on adjacent frequencies can affect the link (Figure 3). Usually, such an influence is not malicious, but it should be considered as a threat, since it can lead to link failure. Our task is to search and select a frequency channel free of interference. Keep in mind that interference may not be present at the installation stage, but may appear during the wireless system operation.

The following actions can reduce the risks associated with this threat:

- **Search for interference sources**: devices of the InfiLINK 2x2, InfiMAN 2x2, InfiLINK Evolution, InfiMAN Evolution families allow you to obtain the MAC addresses of the systems operating in the selected frequency channel using the Radio scanner utility or "muffer" command. It is possible to identify the source of interference and to decide the measures to eliminate its effect on the link.
- **Manual spectrum scan**: manual preliminary radio survey of the territory in which the communication system will be deployed. The frequency is selected taking into account the scanned data. Infinet devices allow to evaluate the state of the spectrum using the built-in "Spectrum analyzer" tool.
- **Auto spectrum scan**: radio survey of the territory in which the communication system is deployed, performed periodically in automatic mode. The frequency channel can be automatically changed in accordance with the scanned data. Infinet devices support the DFS and iDFS technologies (see Dynamic Frequency Selection), which are designed to automatically scan the spectrum.

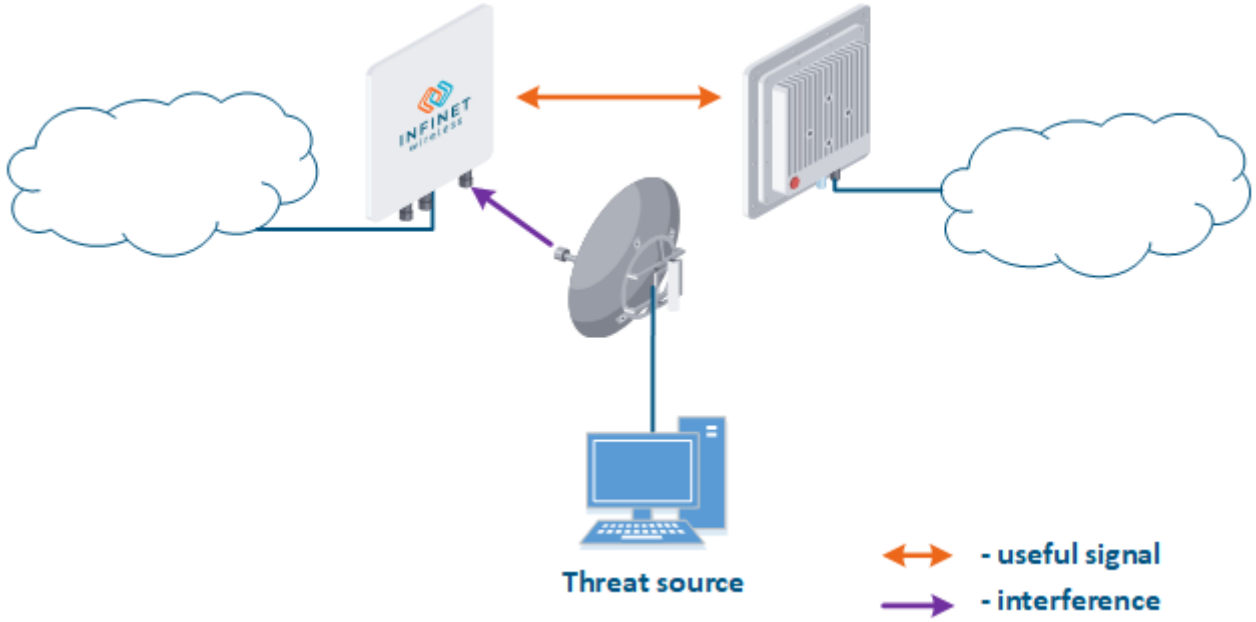

Figure 3 - An example of a threat in the frequency channel

Even if the frequency channels distribution is coordinated, the problem of mutual interference may persist. That happens due to an out-of-band radiation: a radiation spectrum is not an ideal rectangle. It has side bands that affect adjacent frequency channels. Below are the spectra of two communication systems (Figure 4 a-b) using adjacent frequency channels: in the first case (Figure 4a), the radiation power of the systems is equal and the attacking source's influence is lower than the communication system's sensitivity, in the second case (Figure 4b), the radiation power of the attacking source is higher than the one of the communication system and the out-of-band level is higher than the communication system's sensitivity, leading to interference in the communication.

The automatic transmit power control (ATPC) function can help to reduce the influence of a third-party communication system on the used frequency channels. In case of interference, the devices having ATPC active will increase the radiation power and maintain the link performance.

The link budget depends also on the used modulation-coding scheme: higher MCSs require higher link parameters, therefore, they are impossible to use with a low signal level and a high level of interference. Thus, the modulation-code scheme selection is a compromise between the link performance and reliability. The automatic modulation control (AMC) function allows the selection of the modulation-coding scheme according to the current parameters of the radio link. This increases the reliability and the availability of the information, by keeping the link operational even in strong interference conditions.

For more information about signal's frequency characteristics, proceed to the online course "Wireless Networking Fundamentals".

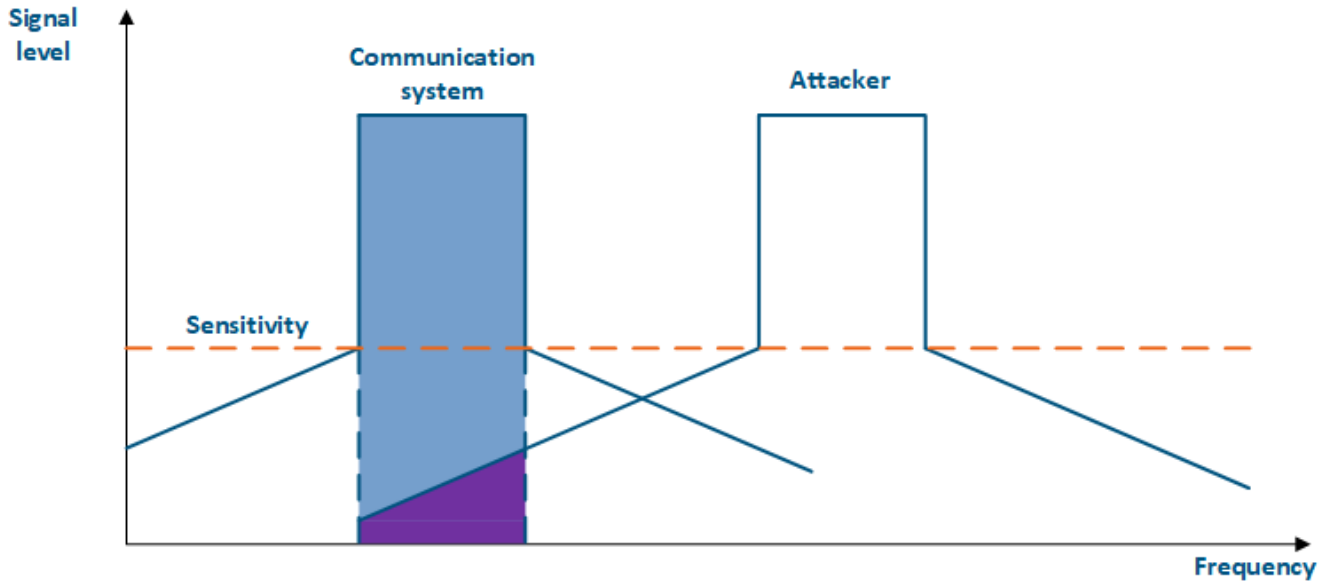

Figure 4a - An example of an adjacent frequency channel influence on a communication system

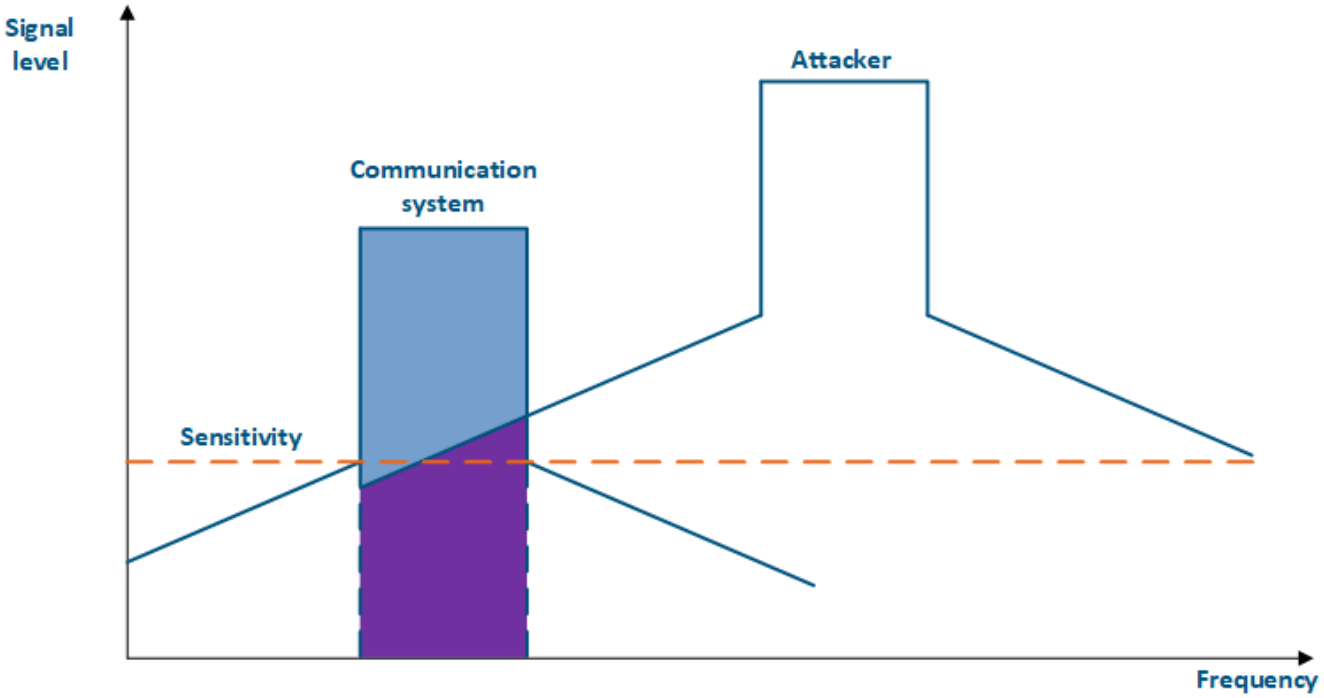

Figure 4b - An example of an adjacent frequency channel influence on a communication system

Authentication Settings

Popular scenarios for the information confidentiality and integrity violation in a radio channel are the attacks of the Man-In-The-Middle type (MITM). Let's look at examples of such attacks:

- **Data interception** (Figure 5a): the attacker installs a device that receives all the transmitted signals in the communication system's coverage area. All wireless systems use a shared data transmission medium, so the devices receive data even if they are not specified as recipients. Further, the device processes the frame at layer 2 if it is the recipient, or discards it, if it is not. An attacker can pretend to be the recipient and gain access to all messages, along with a legal address.
- **Data relay** (Figure. 5b): a specific case of the "Data interception" scenario, in which an attacker uses a relay instead of a passive receiver. Such an attack option is applicable for example for point-to-point links with a narrow radiation pattern, where the Data Interception scenario is not suitable.

- **Data spoofing** (Figure 5c): a specific case of the "Data relay" scenario, in which the attacker changes the data content. In such a scenario, not only confidentiality is violated but data integrity as well.

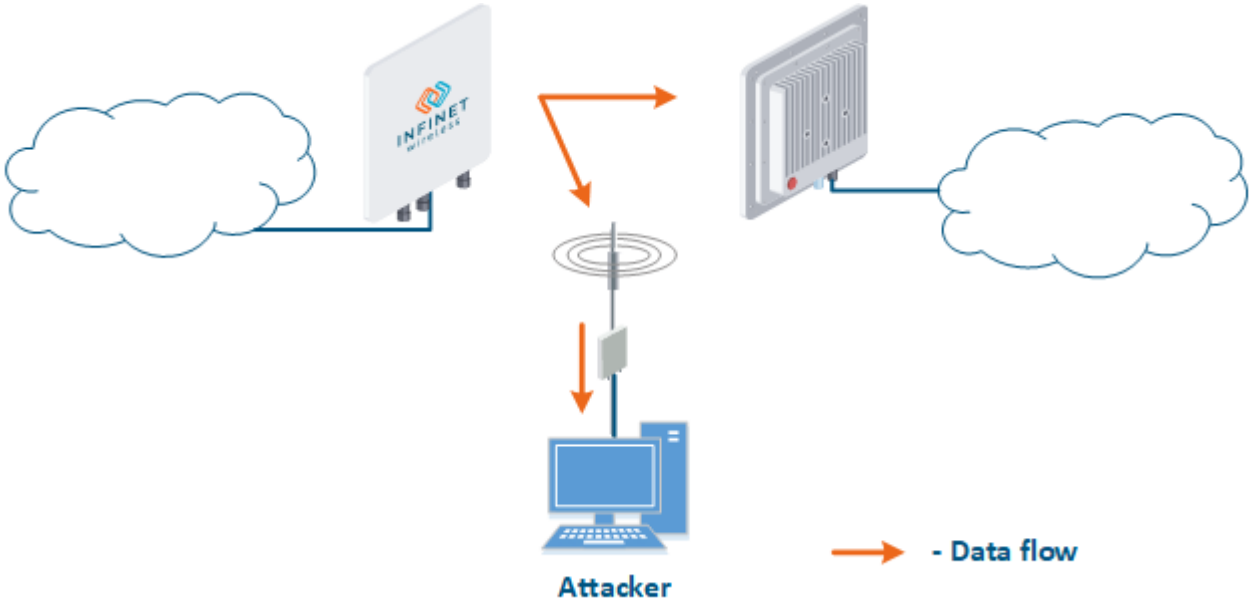

Figure 5a - Data interception

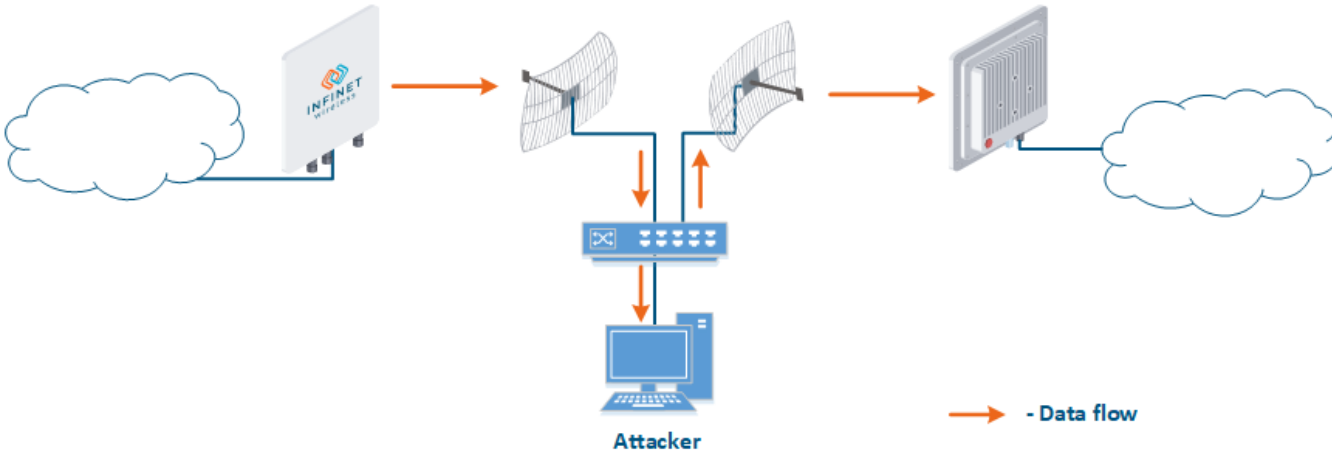

Figure 5b - Data relay

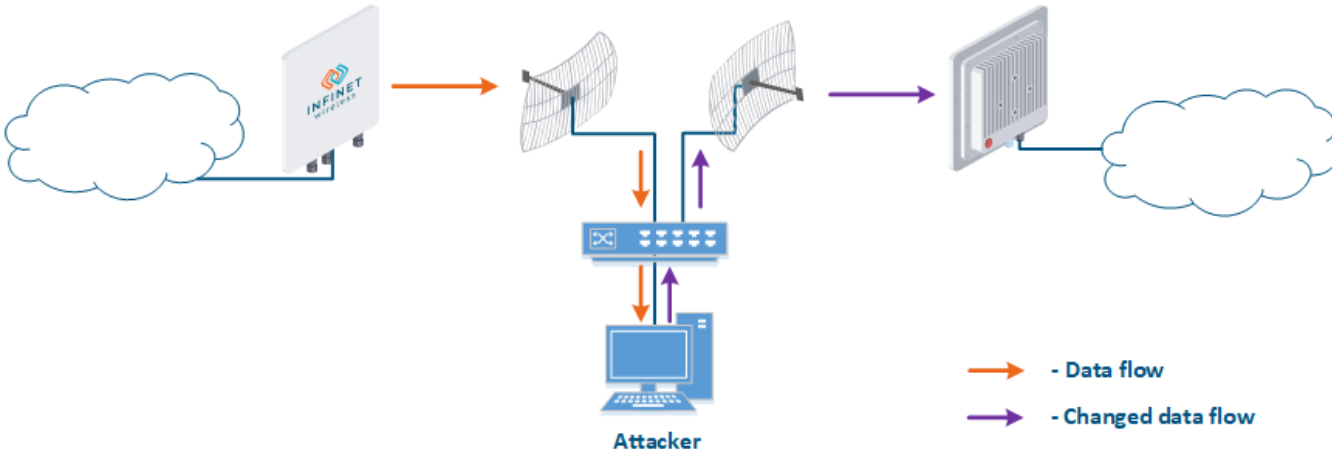

Figure 5c - Data spoofing

There are also possible scenarios in which unauthorized access to the resources can be obtained through a connection to a radio network. Let's look at examples of such attacks:

- **Connection to an enterprise network** (Figure 6): an attacker with a subscriber device can install it in the base station coverage area. After establishing a link with the base station sector, an attacker can gain access to the enterprise network and implement attacks aimed at integrity, availability and confidentiality violation. An attacker will be able to establish a link with a base station sector only if an Infinet wireless device is used.

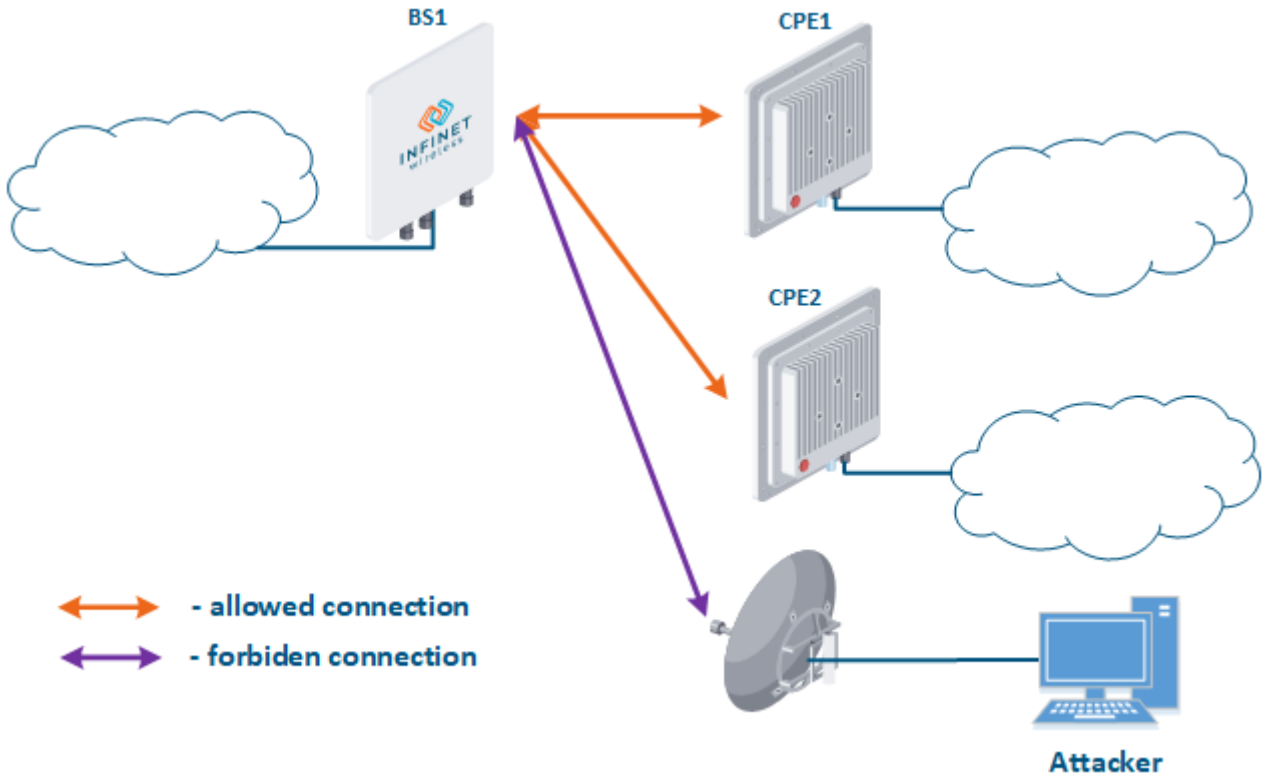

Figure 6 - Connection to an enterprise network

- **Base station sector substitution** (Figure 7a-b): an attacker installs a base station sector to which a subscriber station can connect. After that the attacker gains unauthorized access to the data originating from the subscriber station and to the network segment behind the subscriber station. Let's look at examples of such an attack in scenarios using mobile objects (see Connectivity with mobile objects). A radio link is established between BS1 and the CPE (Figure 7a). The CPE is installed on the mobile object and breaks the connection while moving away from BS1 and starts to look for a new base station sector to establish a connection (Figure 7b). An attacker inserts a base station sector along the CPE's route, between BS1 and BS2, therefore, after disconnecting from BS1, the CPE establishes a connection with the attacker's sector. This attack type implementation is only possible in case of disregarding the security settings.

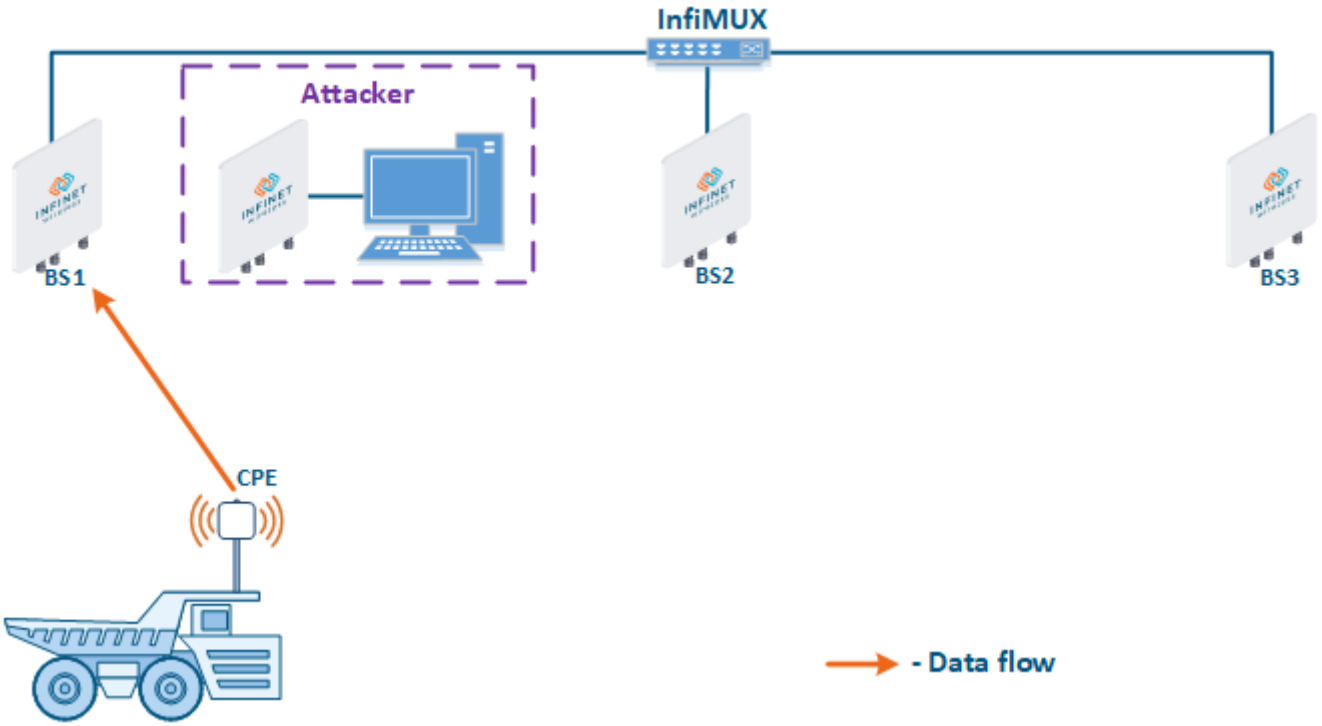

Figure 7a - Connection of the CPE to the enterprise base station sector

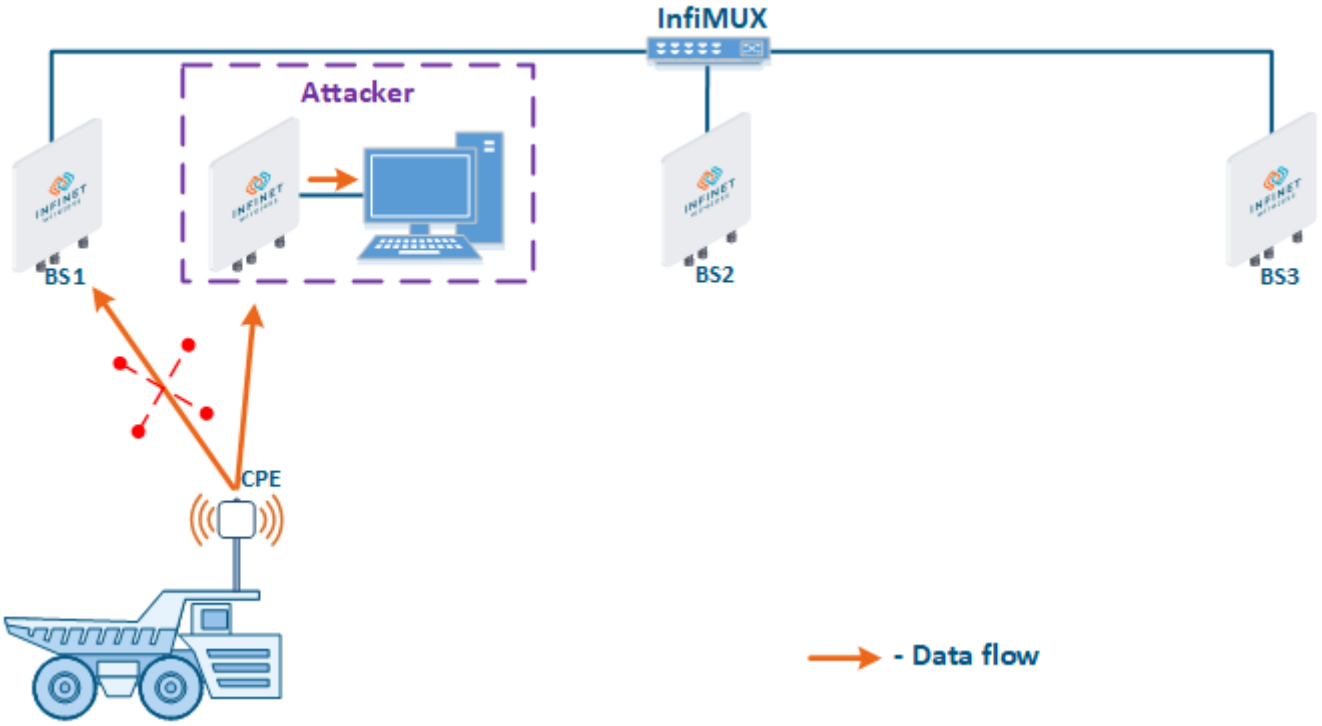

Figure 7b - Connection of the CPE to the attacker's base station sector

The Infinet devices use their own radio frame format, making it impossible to establish communication with any devices operating according to the 802.11 family standards. This complicates the attacker's plans, as he will be forced to use Infinet devices.

To counter such attacks, the following options should be used:

- **Link ID:** always change the default value to unique.

- **Security key:** devices can establish a connection only if they have the same link ID and security key, i.e. in order to reduce the likelihood of establishing a link with an attacker's device, security keys must be installed on both devices.
- **Authentication Mode:** The InfiLINK 2x2, InfiMAN 2x2, InfiLINK Evolution, InfiMAN Evolution family devices support authentication mode settings when establishing a wireless link. "Static" and "remote" modes can limit the list of devices with which the link establishment is allowed. The static mode allows to configure a list of MAC addresses of the devices with which a connection can be established (white list), or a list of addresses with which the connection establishment is forbidden (black list). The remote method allows to store MAC addresses for whitelists or blacklists centrally and perform appropriate requests when trying to establish a connection. Using one of the described authorization methods will significantly complicate an unauthorized connection of an attacker to the network.
- **Max links:** sets the maximum allowed number of connected CPEs. It is recommended to set the value of the actual subscriber stations number.
- **Scrambling:** reversible process of redistributing the data bits according to a given algorithm in order to equalize the frequency spectrum of the signal. Scrambling also makes it difficult to decrypt the intercepted data, because the attacker must know the scrambling algorithm that was used in order to recover the original bit sequence. The scrambling/descrambling operations will require hardware resources, therefore it is recommended to use this option in cases of low hardware load.
- **Frequency grid:** the frequency range supported by the radio module can be deliberately limited using the frequency grid on all Infinet devices. This restriction narrows down the list of frequencies that can be set as central. The frequency grid additional effect is to increase the level of protection against choosing a random frequency channel as operational. If the automatic center frequency selection is set, then the device will select it according to the grid. The center frequency can be set manually: on Master devices, the center frequency is set strictly, on Slave devices, depending on the family, either strictly or using one or more radio profiles. If a subscriber station uses several radio profiles (see Connectivity with mobile objects), then in order to connect to the base station sector, the profiles will be scanned until finding a parameter match.
- **Global function:** in scenarios with mobile objects, the Global option is used to connect a subscriber station to base stations sectors that are connected to the network core (see Connectivity with mobile objects). This approach can be used to block the CPE connections to base stations sectors installed by attackers (Figure 7b): since the attacker's base station is not connected to the network core, the subscriber station will ignore the attacker device during roaming.

Implementation of strategies for radio link security

Radio link safety measures

Measures	InfiLINK 2x2 and InfiMAN 2x2		InfiLINK Evolution and InfiMAN Evolution		InfiLINK XG and InfiLINK XG 1000		Quanta 5 and Quanta 6	Quanta 70
	Web	CLI	Web	CLI	Web	CLI	Web	Web
Spectrum analysis	Spectrum Analyzer	Muffer command	Spectrum Analyzer menu	Muffer command	Spectrum Analyzer	Command for spectrum scanning	Spectrum Analyzer	-
Radio Scanner	Device status	Muffer command	-	Muffer command	-	-	-	-
DFS technology support	Link Settings	dfs (Dynamic Frequency Selection)	Link Settings	dfs (Dynamic Frequency Selection)	Radio settings	Commands for modem configuration	Radio settings	Radio settings
Instant DFS technology support	Link Settings	mint command in MINT version mint command in TDMA version	Link Settings	mint command in TDMA version	Radio settings	Commands for modem configuration	-	-
DFS/Instant DFS work results	DFS menu	-	DFS menu	-	Instant DFS	Commands for modem configuration	-	-
Automatic transmission power control	Link Settings	rfconfig command in MINT version rfconfig command in TDMA version	Link Settings	rfconfig command in TDMA version	Radio settings	Commands for modem configuration	Radio settings	Radio settings
Automatic MCS control	Link Settings	rfconfig command in MINT version rfconfig command in TDMA version	Link Settings	rfconfig command in TDMA version	Radio settings	Commands for modem configuration	Radio settings	Radio settings
Link ID	Link Settings	rfconfig command in MINT version rfconfig command in TDMA version	Link Settings	rfconfig command in TDMA version	Radio settings	Commands for modem configuration	General settings	General settings
Link security key	Link Settings	mint command in MINT version mint command in TDMA version	Link Settings	mint command in TDMA version	Radio settings	Commands for modem configuration	Security settings	Security settings
Authentication mode configuration	Link Settings	mint command in MINT version mint command in TDMA version	Link Settings	mint command in TDMA version	-	-	-	-

Lists for static authentication mode	Static Links	mint command in MINT version mint command in TDMA version	Static Links	mint command in TDMA version	-	-	-	-
Lists for remote authentication mode	-	mint command in MINT version mint command in TDMA version	-	mint command in TDMA version	-	-	-	-
Maximum number of subscriber stations	Link Settings	mint command in MINT version mint command in TDMA version	Link Settings	mint command in TDMA version	-	-	-	-
Scrambling technology	Link Settings	mint command in MINT version mint command in TDMA version	Link Settings	mint command in TDMA version	-	-	-	-
Frequency grid configuration	Link Settings	rfconfig command in MINT version rfconfig command in TDMA version	Link Settings	rfconfig command in TDMA version	Radio settings	Commands for modem configuration	Radio settings	Radio settings
Central frequency configuration (for Master device)	Link Settings	mint command in MINT version mint command in TDMA version rfconfig command in MINT version rfconfig command in TDMA version	Link Settings	mint command in TDMA version rfconfig command in TDMA version	Radio settings	Commands for modem configuration	Radio settings	Radio settings
Central frequency configuration (for Slave device)	Link Settings	mint command in MINT version mint command in TDMA version rfconfig command in MINT version rfconfig command in TDMA version	Link Settings	mint command in TDMA version rfconfig command in TDMA version	Radio settings	Commands for modem configuration	Radio settings	Radio settings
Regulatory domain	-	-	-	-	-	-	General settings	General settings
Global function	-	mint command in MINT version mint command in TDMA version	-	mint command in TDMA version	-	-	-	-

Device management

The unauthorized access to the device's management interface is a serious threat that can lead to a violation of all the basic data properties. Measures to ensure the information security and to reduce the potential risks should be elaborated carefully.

Authentication and Authorization

CAUTION

By default, one user is added to the configuration with administrative rights and with the following login values:

- **login:** any nonempty string;
- **password:** any nonempty string.

Since the default authentication settings allows a high probability of unauthorized access, change the username and password during initial setup.

A company can have several lines of technical support: in such a scheme, some problems that do not require wireless device reconfiguration can be solved by the first line of technical support. Thus, trivial tasks can be solved without qualified employees of the second and third lines of technical support. To implement this scenario, a guest account can be added to the device's configuration. A user which has access to the management interface using a guest account can use the tools and view interface statistics, but it is not allowed to make configuration changes.

It is recommended to use a centralized account storage for networks having a large number of devices. This allows to avoid errors when blocking accounts, provides a single password policy and have a single interface for account management. Infinet devices support the RADIUS protocol, which is intended for

centralized authentication, authorization and account management in networks. Depending on the capabilities and on the scale of the network, the database for the RADIUS operation can be deployed on a separate device, or combined with other network elements.

The algorithm for a RADIUS server usage is the following (Figure 8):

1. **Request to access the device's management interface:** the user tries to access the device's management interface using one of the protocols (see below), by forming a request with username and password included.
2. **Forming a request to the RADIUS server:** the device receives a request from the user and generates a request to the server in accordance with the RADIUS protocol.
3. **RADIUS server reply:** the RADIUS server receives the request and checks for the presence and rights allocated to the user whose credentials are passed in the request. The server can answer in two ways:
    a. **Access is allowed:** the account is present in the database and it is allowed to access the Slave's device management interface (Figure 8a).
    b. **Access is denied:** the account is absent in the database, or access to the Slave's management interface is denied for this user (Figure 8b).
4. **Device decision making:** the device receives a response from the RADIUS server and makes a decisions about the user authorization. In case of successful authorization, the user will go further to the device's management interface (Figure 8a), otherwise, the user connection is reset and an information message is displayed.

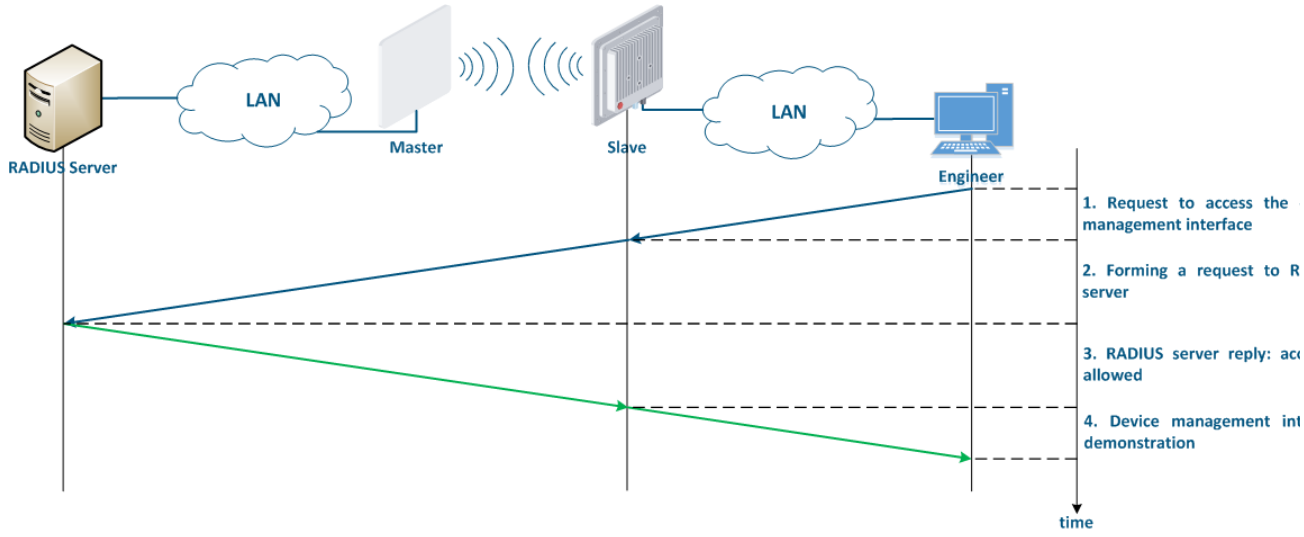

Figure 8a - An example of successful RADIUS authentication

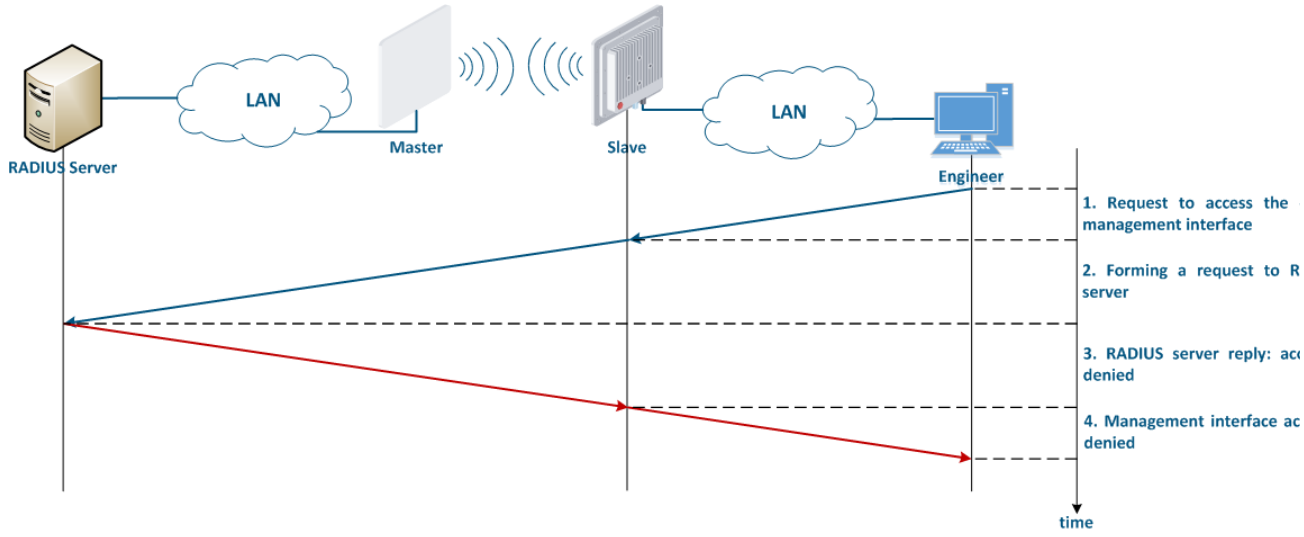

Figure 8b - An example of unsuccessful RADIUS authentication

Access methods

Infinet devices can be configured using the Web GUI or the command line interface (CLI). Some parameters can only be configured via CLI. Access to different interfaces is carried out using various network protocols. It is recommended to disable the unused protocols, in order to reduce the probability of unauthorized access to the device's management interface.

The management protocols supported by the Infinet devices correspond to the management interfaces in the following way:

- **Web GUI:**
  - **HTTP:** data is transmitted over the network unencrypted, so an attacker, gaining access to the network, can intercept it.
  - **HTTPS:** data is transmitted over the network encrypted, so an attacker who intercepts the data will not be able to decrypt it without the corresponding encryption keys. Unless there are specific reasons for using HTTP, the HTTPS protocol should be used.
- **CLI:**
  - **Telnet:** data is transmitted over the network unencrypted, so an attacker, gaining access to the network, can intercept it. The telnet protocol is acceptable in case of emergency, when there is no possibility of using SSH.
  - **SSH:** data is transmitted over the network encrypted. In case that an attacker intercepts the data, he will not be able to decrypt it without the corresponding encryption keys.

Network management interface

The network management interface (mgmt), which is used to access the device is structured differently, depending on the device families:

- **InfiLINK XG, InfiLINK XG 1000, Quanta 5, Quanta 6 and Quanta 70:** for device management an internal virtual interface is allocated, which can be associated with an IP address.
- **InfiLINK 2x2, InfiMAN 2x2, InfiLINK Evolution and InfiMAN Evolution:** an IP address can be associated with virtual or physical interfaces, i.e. various interfaces can act as a network management interface, for example eth0, svi100. Several network management interfaces of the same or of different types can be added to the configuration.

In addition to selecting the management interface, it is also possible to control the connectivity between the management interface and the other network interfaces. This mechanism allows to restrict the access to the device via wired or wireless interfaces, depending on the scenario.

Figure 1 shows some practical scenarios when using Infinet devices. Let's look at the device management configuration for each scenario. In this sense, we have added PCs to different network segments in order to perform the management configuration (Figure 9a-c):

- **Joining of internal network segments:** access to the devices' management interfaces should be provided to PC users from different network segments (Figure 9a). The wireless devices are located on the internal network and do not directly contact the external network devices. The function of protecting against unauthorized access should be performed by the network elements located at the border between the internal and the external networks.
- **Connection of the internal and the external network segments:** access to the device's management interface should be granted only to a PC user connected to the local network segment (Figure 9b), i.e. the ability to transfer data between the management interface and the Slave's device wired interface should be disabled.
- **Connection of the internal network segment with the Internet:** access to the device's management interface should be granted only to a PC user connected to the local network segment (Figure 9c). In addition, access may be granted to some PC users connected to the Internet. In this case, incoming traffic filtering must be configured on border devices, as it is shown below.

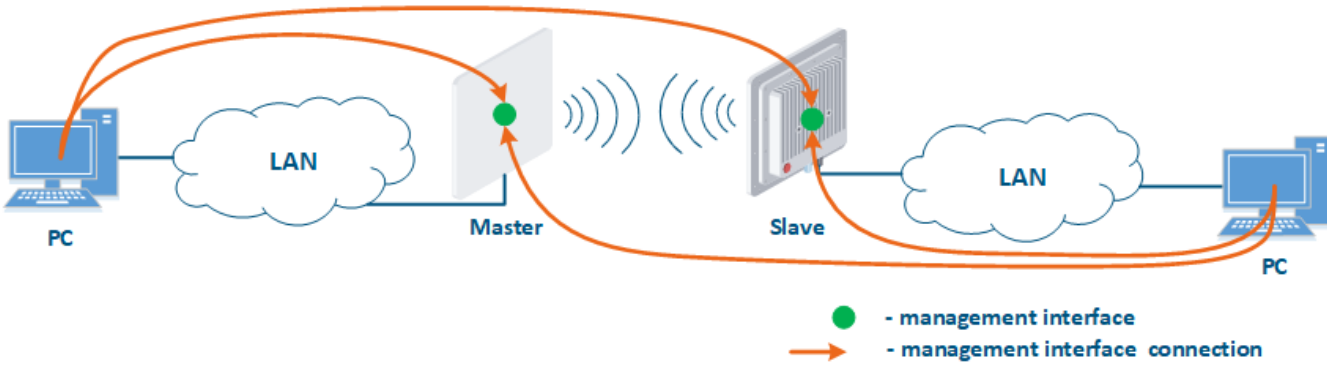

Figure 9a - Radio link joining internal network segments

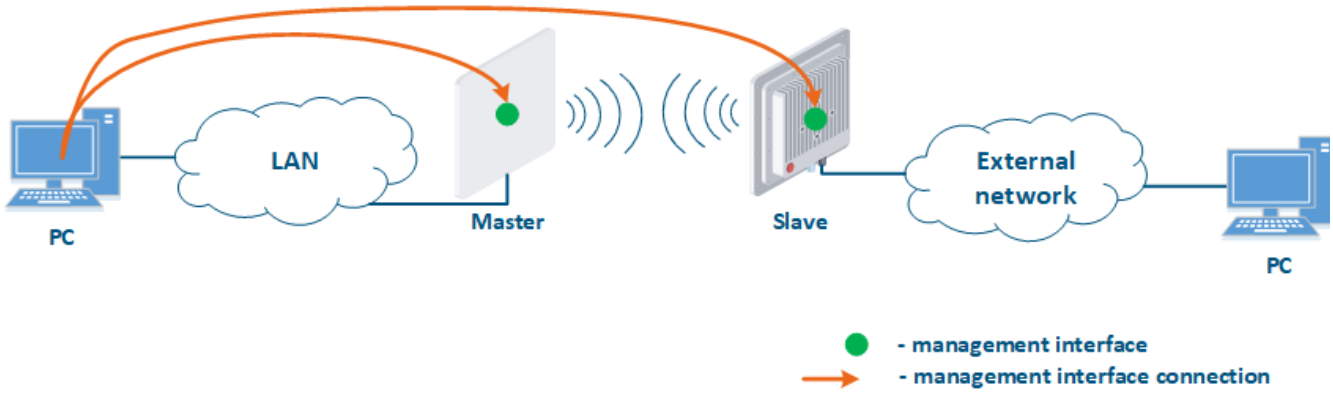

Figure 9b - Radio link connecting internal and external network segments

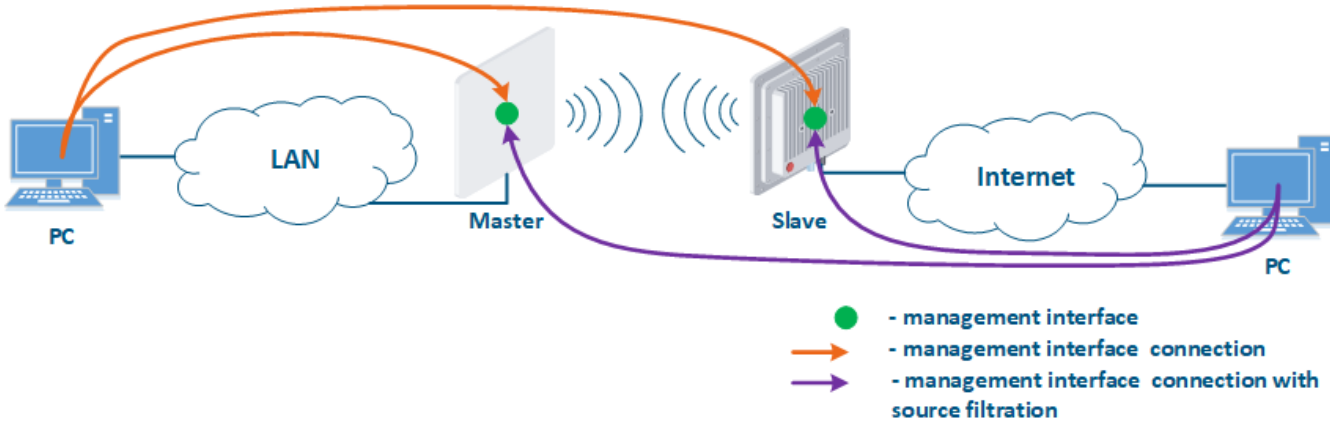

Figure 9c - Radio link connecting an internal network segment with the Internet

We recommend to use the following principles of management configuration:

- Use the virtual interface as management interface:
  - InfiLINK XG, InfiLINK XG 1000, Quanta 5, Quanta 6 and Quanta 70 family devices: network management interface (mgmt).
  - InfiLINK 2x2, InfiMAN 2x2, InfiLINK Evolution and InfiMAN Evolution family devices: svi network interface attached to the management switch group.
- Access to the management interface should be allowed only through the network interfaces connected to the engineers' PC or through the services that manage devices, for example, a monitoring system.
- In the case of network traffic isolation using a VLAN, a separate VLAN must be allocated for the management traffic and associated with the management interface.

Access limitation

IInfiLINK 2x2, InfiMAN 2x2, InfiLINK Evolution, Quanta 5, Quanta 6 and Quanta 70 family devices allow to create white access lists. In this case, only the network nodes whose IP addresses are mentioned in the list will be permitted to access the management interface.

Access recovery

The ERConsole utility is used to restore the access to all Infinet devices (see the "ERConsole" screencast). The tool can be used for the following purposes:

- **Error in the device's configuration:** the ERConsole tool allows to assign an IP address to the interface, or reset the device to factory settings in case of fatal errors in configuration.
- **Device protection against an attacker:** To reset the Infinet device to the factory settings, a factory password is required, which is assigned to the company that purchased it. If the device is stolen by an attacker, he will not be able to get the factory password from the technical support, because he is not an employee of the enterprise, which means he will not be able to access the device.

Security measures implementation in device management configuration

Security measures for device management

Measures	InfiLINK 2x2 and InfiMAN 2x2		InfiLINK Evolution and InfiMAN Evolution		InfiLINK XG and InfiLINK XG 1000		Quanta 5 and Quanta 6	Quanta 70
	Web	CLI	Web	CLI	Web	CLI	Web	Web
Change account settings	System Settings	General Purpose Command Set	System Settings	General Purpose Command Set	General settings	General Purpose Command Set	Security settings	Security settings
Create a guest account	-	General Purpose Command Set	-	General Purpose Command Set	General settings	General Purpose Command Set	-	-
Authentication via RADIUS Server	-	General Purpose Command Set RADIUS authentication for admin users	-	General Purpose Command Set RADIUS authentication for admin users	-	General Purpose Command Set	Security settings	Security settings
Management protocol configuration	Maintenance menu	td command (Telnet daemon) General Purpose Command Set	Maintenance menu	td command (Telnet daemon) General Purpose Command Set	General settings	td command (Telnet daemon) General Purpose Command Set	Security settings	Security settings
Adding a management IP	Network Settings	Ifconfig command (interfaces configuration)	Network Settings	Ifconfig command (interfaces configuration)	Network Access	Ifconfig command (interfaces configuration)	Network settings	Network settings
Device access limitation	IP Firewall	General Purpose Command Set ipfw command (IP Firewall)	IP Firewall menu	General Purpose Command Set ipfw command (IP Firewall)	-	-	Security settings	Security settings
Device access recovery	Emergency Repair Console	General Purpose Command Set	Emergence Repair Console	General Purpose Command Set	Emergency Repair Console		Troubleshooting	Troubleshooting

Data transmission

Data transmission is the main function of any network equipment. In addition to user data, the devices exchange service messages of auxiliary protocols such as SNMP, LLDP, etc. The different's protocols design contains potential threats that an attacker can use and requires accurate configuration of all the wireless device subsystems.

General recommendations

Wireless systems are hardware and software systems. Therefore, one of the most important requirements is the timely software updating. It is recommended to use stable software versions and monitor the release of updates. The current software version can be checked directly on the device.

When making changes to the device's configuration, keep in mind that the mechanism for applying the settings depends on the used management interface:

- **Web GUI:** changes made in different sections of the interface are accumulated and sequentially added to the configuration only after clicking the "Apply" button. When the device is rebooted, the last successfully saved configuration will be loaded.
- **CLI:** the command is instantly added to the current configuration, but not saved. To save the settings, run the appropriate command. When the device is rebooted, the last successfully saved configuration will be loaded.

In some cases, errors made during the device's configuration process can lead to losing access and the device may need to be reset to factory settings (see "Access recovery"). To reduce the risk of this scenario, it is recommended to use a delayed device reboot. In this case, after applying the new configuration, a device availability check will be performed. If the device is unavailable, the previous version of the configuration will be restored.

Service traffic

By default, switching on the device is configured to pass data between the wired and wireless interfaces without any filtering. Such a scheme is vulnerable to a large amount of spurious traffic, which can take up all the available throughput and the link will actually become inaccessible for the transmission of useful traffic. An example of spurious traffic is a broadcast storm, which can cause errors in switching. The measures to protect the network infrastructure from such attacks are:

- **Traffic filtering:** a good practice is to split the physical infrastructure into multiple virtual local area networks using the VLAN technology. This method allows to limit broadcast domains, and thus reduce the impact of a broadcast storm. This will require traffic filtering of different VLANs on devices: for wireless devices it is recommended to allow only those VLAN tags that really should be transmitted through the radio link and deny all the others.
- **STP:** Spanning Tree Protocol is designed to prevent link-level loops that could cause a broadcast storm. In addition, the STP protocol can be used to build automatic backup schemes at L2 layer in networks with redundancy.

- **Router mode:** Routing can reduce the size of the broadcast segment that will lead to a lower impact of the broadcast storm. A router is a device that divides broadcast domains, i.e. a broadcast storm in one domain will not affect the operation of the devices in another domain. Routing also involves the packet transmission based on the IP header with a TTL field included, which prevents packets from cycling through the network.

Network Protocol Configuration

In addition to user data, the devices exchange service messages of auxiliary protocols. The security policy should take into account that any available service is a potential attacker's target.

DHCP

Infinet devices can be configured as a DHCP client, DHCP server or DHCP relay. Keep in mind that the DHCP protocol supports not only the IP address allocation, but also the network settings transmission.

Let's look at the example of an attack using DHCP (Figure 10): a link is established between the Master and Slave, a DHCP client is activated on the Slave's device radio interface and the DHCP server is installed on the corporate network. In this example the attacker managed to connect to the network device on which the DHCP server is configured within the corporate network. After the Master-Slave link has been established, the Slave device sends a broadcast request to the network to receive the network settings from the DHCP server. The DHCP servers located on the network respond to the request from Slave. If the response from the attacker server is received first, the Slave device will assign to the network interface the proposed address and network settings that are transmitted in this request. Thus, an attacker can set his device as the default router and gain access to the traffic transmitted by the Slave device.

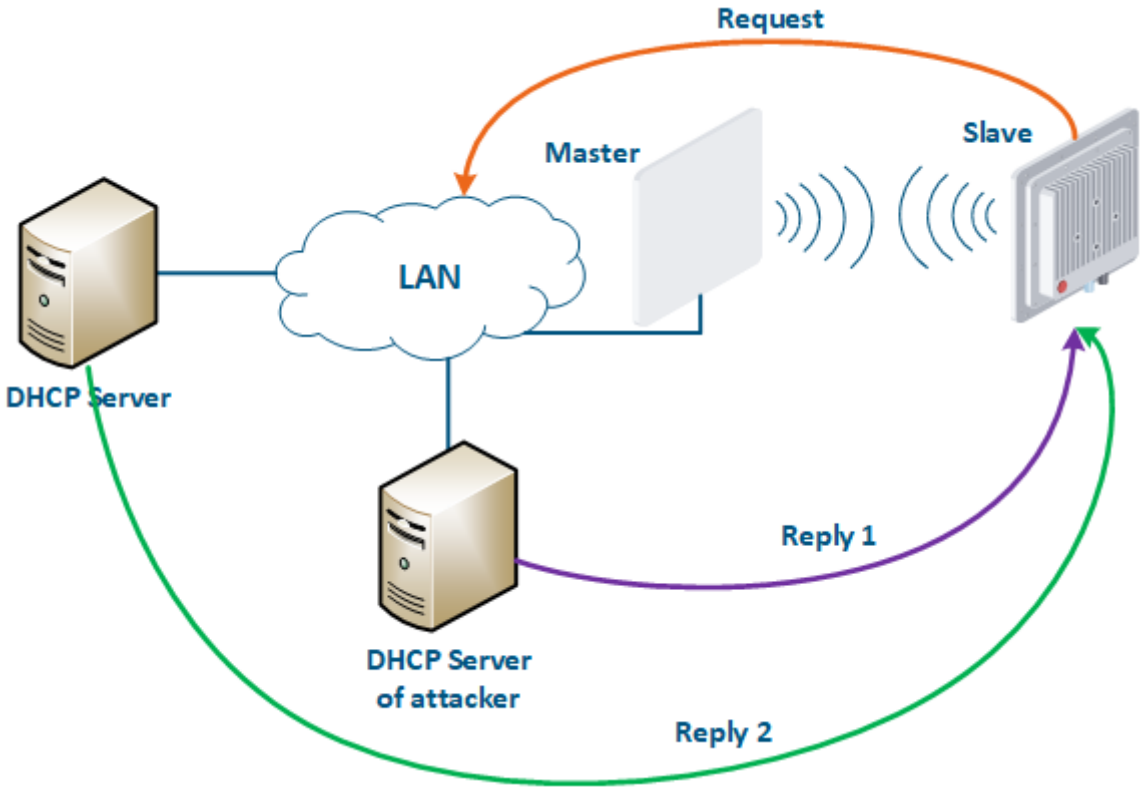

Figure 10 - An example of attack using DHCP

An attacker’s device can also act as a DHCP client (Figure 11): the DHCP server is implemented on the Infinet device, while an attacker’s device is connected to the network. In a situation where the DHCP server configuration protocol does not provide security measures, the attacker will generate a request and the server will provide the device with the network details. Thus, an attacker will gain access to data transmitted over the network.

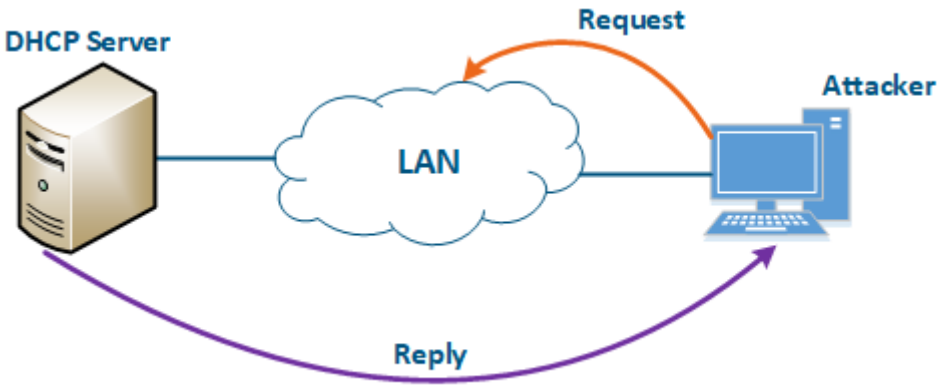

Figure 11 - An example of attack using DHCP

In order to increase the security when using DHCP in a corporate network, it is recommended to implement the following measures:

- **DHCP servers list limitation at the DHCP client:** The DHCP client allows to limit the list of servers for which a network settings request will be generated. In this case, the DHCP client will generate requests for the specified DHCP servers, if they do not respond, it will generate a broadcast request.
- **Security key usage:** a security key can be used during the client authentication. Keep in mind that this setting must be performed both on the DHCP server and on the DHCP client.
- **Client-address pair in a DHCP server configuration:** the DHCP server configuration allows to record the IP addresses allocated to clients. Thus, it is possible to create white lists of devices, so that obtaining the network details will become complicated for an attacker.
- **DHCP Snooping:** this technology allows to prevent receiving network details from the attacker's DHCP server. The operation principle is very simple: the Ethernet ports, behind which the DHCP server is located, are marked as trusted, the rest as untrusted. Messages from DHCP servers that arrived at the untrusted ports will be discarded, which makes it impossible for client devices to obtain network details from the attacker's server.
- **Disable DHCP on unused interfaces:** the list of interfaces on which DHCP is enabled should be carefully monitored. Disable DHCP on interfaces that are not used for data transfer or use static addressing. This recommendation is for both the DHCP client and the DHCP server.
- **Static configuration:** keep in mind that the DHCP usage must be limited, a lot of scenarios require a static assignment of the network settings to the corresponding interfaces. For example, it is recommended to assign static addresses to key network elements, which may include Infinet wireless devices. This will help to avoid problems in organizing technical accounting and monitoring systems.

ARP

The Ethernet and the IP protocols belong to different layers of the network interaction model.In order to bind the addresses of the devices used by each protocol, a special protocol is needed. ARP with its address mapping table are used for this purpose. The table contains entries where the MAC address of the interface is mapped to the IP address that is used when transmitting IP packets encapsulated in Ethernet frames.

Let's look at an example of attack using IP address spoofing: two clients (Client 1 and Client 2) have access to the Internet via the Master-Slave radio link. The IP address assigned to the client is an identifier for the appointment with a tariff plan. The client with the IP address 192.168.0.1 is provided with a throughput of 10 Mbit/s, the client with the address 192.168.0.2 - with 2 Mbit/s (Figure 12a). At some point Client 1 turns off the PC and does not use the provider services, at the same time Client 2 replaces its IP address with the 192.168.0.1 address assigned to Client 1 (Figure 12b). In this case Client 2 will gain access to the Internet with greater throughput, and Client 1 after switching on, will have problems in accessing the network.

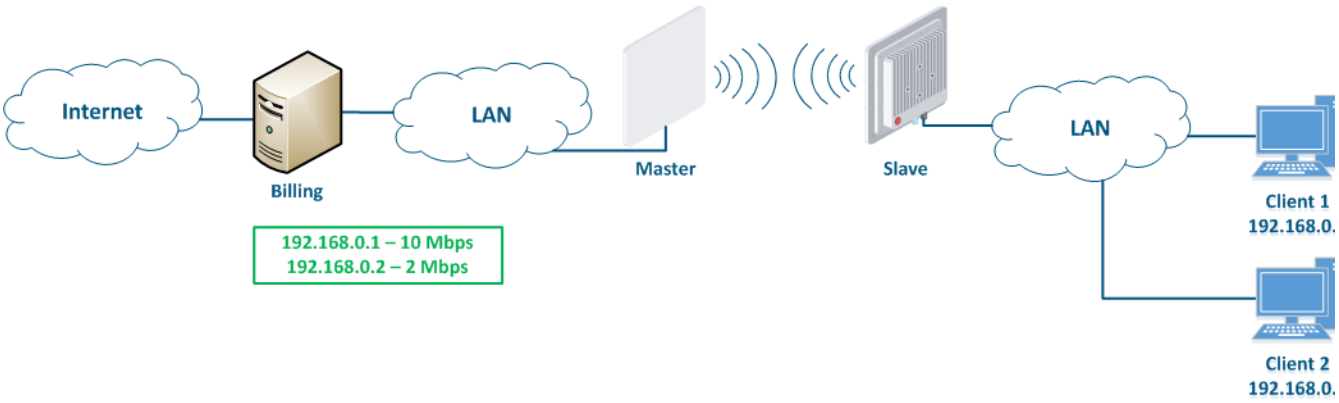

Figure 12a - An example of attack using IP spoofing

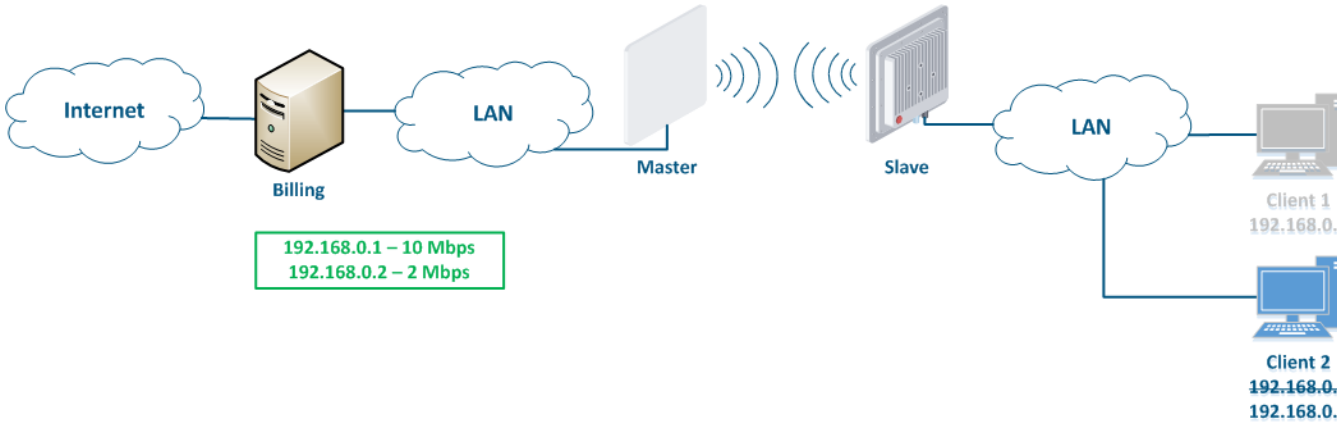

Figure 12b - An example of attack using IP spoofing

This type of attack can be prevented by adding a static record to the ARP protocol address mapping table. In this case, Client's 2 data will not be transmitted after changing the IP address, because the address 192.168.0.1 is assigned to the MAC address of Client 1.

LLDP

The LLDP protocol is designed to exchange service information about a device with its directly connected devices. The service information can be the VLAN ID, the MAC address, the device's name, the IP address of the management interface, etc. If an attacker will gain physical access to the device, then by launching the LLDP service on his PC, he will be able to obtain information about the device by exchanging service messages (Figure 13). This information can help the attacker to get unauthorized access to the device.

To prevent this type of attack, follow these guidelines:

- **Global LLDP disabling:** if the technical policy of the company does not require the LLDP usage, it is recommended to disable its operation on all network devices.
- **LLDP disabling on interfaces:** if it is necessary to use LLDP, then it should be allowed only on those network interfaces to which network infrastructure elements are connected.

Figure 13 - An example of attack using LLDP

SNMP

SNMP was created as a unified protocol for managing network devices and collecting data about their state. The protocol provides two types of requests: a request to GET some parameter value and a request to SET the specified parameter value. Thus, the devices that support SNMP can operate in read mode (only GET requests) and write mode (SET and GET requests). The SNMP server activation is necessary for centralized device management using a monitoring system. But an attacker could take his chance if the SNMP server is not configured properly. In this case, he can not only get information about the network structure, but also change the configuration of the device (Figure 14).

To prevent unauthorized access follow these guidelines:

- **SNMPv3:** by default, SNMPv1 and SNMPv2c support is activated on the devices - a community with the name "public" is created. The SNMPv1 and SNMPv2c protocols provide authentication using the community name, which is openly transmitted over the network. SNMPv3 is recommended to be used due to the implementation of authentication and of message encryption.
- **Read only mode:** if the SNMP SET mode is not used, then its support must be disabled. This will reduce the potential consequences of unauthorized access.
- **White lists:** Infinet devices allow to create white lists of access to the SNMP server.

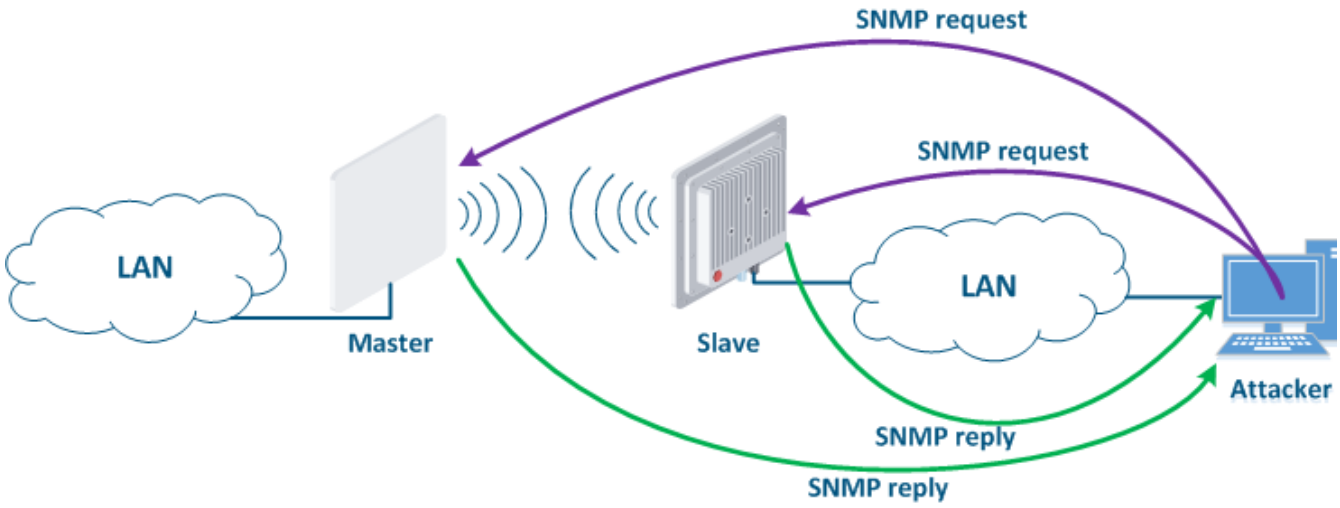

Figure 14 - An example of attack using SNMP

MINT

MINT is the proprietary Infinet protocol, whose operation can be organized in the wired and in the wireless segments. An attacker, gaining access to the MINT domain, can compromise all network devices connected to this domain, therefore, pay special attention when configuring the MINT protocol.

Let's look at the example of an attack using the MINT protocol: two wireless links Master 1 - Slave 1 and Master 2 - Slave 2 are joined into a MINT area using PRF interfaces (Figure 15a). The attacker gets physical access to the enterprise network using the InfiMUX switch, on which a PRF interface is created (Figure 15b). PRF interfaces will establish communication channels between each other and all devices will be joined into a MINT area, so an attacker will receive information about the devices in this area and will be able to execute remote commands on them using MINT tools.

Protection against such attacks:

- **Security key:** the PRF interface is a virtual radio interface operating in a wired environment, therefore, same as for wireless interfaces, the PRF interface supports the ability to configure a security key. In this case, the link between two PRF interfaces will be established only if their security keys match.
- **Password for remote commands execution:** one of the MINT protocol tools is the ability to remotely execute commands on a device located in the same MINT area. By default, remote command execution is available without a password. Set a password to limit the rights of the attacker.

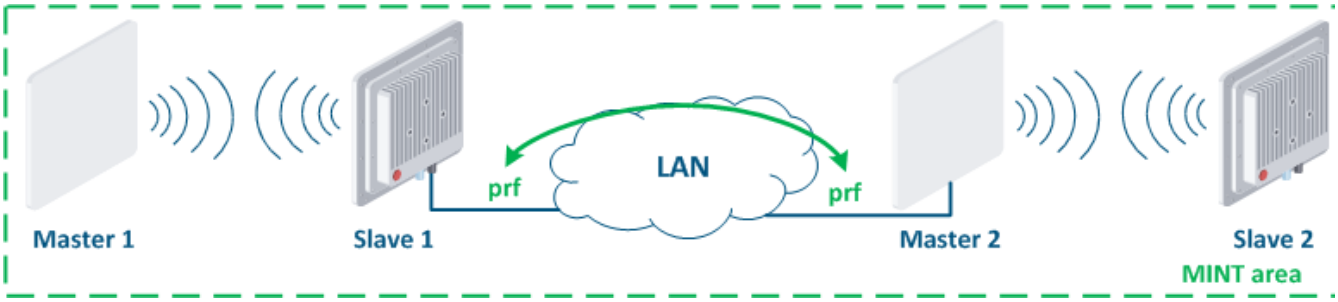

Figure 15a - Joining links in the MINT area

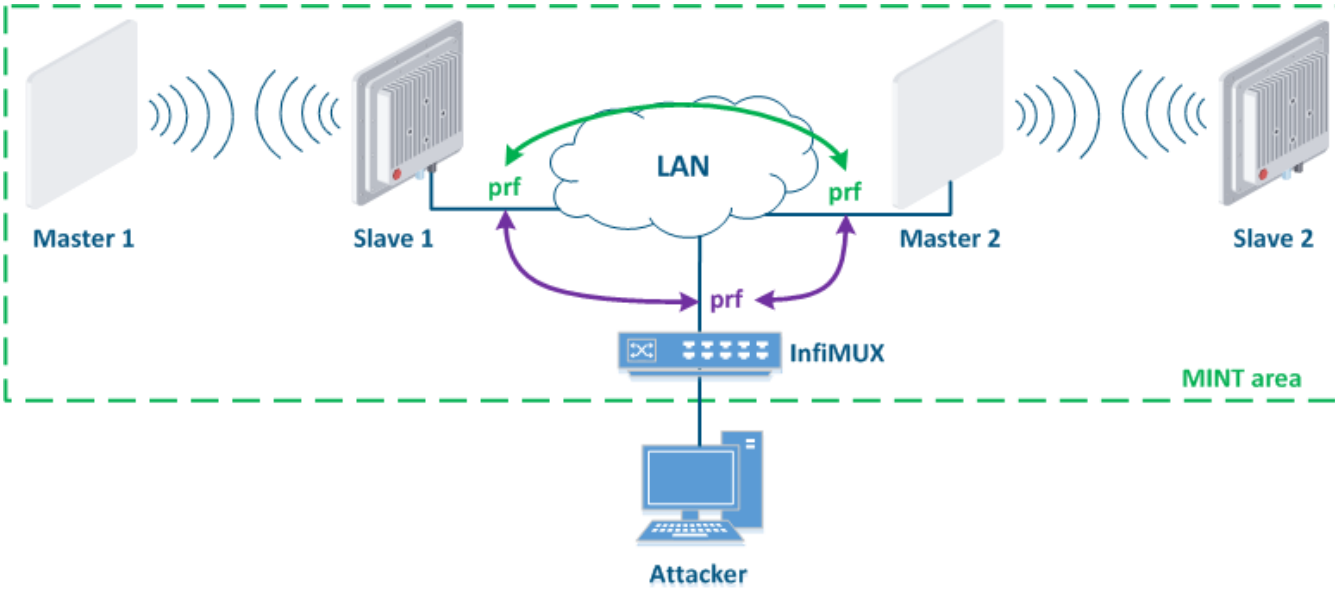

Figure 15b - An example of attack using the MINT protocol

Security measures implementation for data transfer

Implementation of the security measures for data transfer

Measures	InfiLINK 2x2 and InfiMAN 2x2		InfiLINK Evolution and InfiMAN Evolution		InfiLINK XG and InfiLINK XG 1000		Quanta 5 and Quanta 6	Quanta 70
	Web	CLI	Web	CLI	Web	CLI	Web	Web
Software Update	Maintenance	General Purpose Command Set	Maintenance menu	General Purpose Command Set	Maintenance	General Purpose Command Set	Maintenance	Maintenance
Delayed restart	Apply, Try and Preview buttons for the configuration	General Purpose Command Set	Basic Settings	General Purpose Command Set	Apply and Try buttons	Commands for modem configuration	-	-
Traffic filtering	IP Firewall MAC Switch	IP Firewall PCAP-filters Switch command	IP Firewall menu MAC Switch	IP Firewall PCAP-filters Switch command	Switch VLAN Switching	Commands for switch configuration	Switch Settings	Switch Settings
STP configuration	MAC Switch	Switch command	MAC Switch	Switch command	-	-	-	-
Router mode enabling	-	Static routes arip command OSPF command ARDA (Aqua Router DAemon)	-	Static routes arip command OSPF command ARDA (Aqua Router DAemon)	-	-	-	-
DHCP client configuration	Network Settings	DHCP Client	Network Settings	DHCP Client	Network Access	DHCP Client	Network settings	Network settings
DHCP server configuration	-	DHCP Server	-	DHCP Server	-	-	-	-
DHCP relay configuration	-	DHCP relay	-	DHCP relay	-	-	-	-
ARP configuration	-	ARP protocol Addresses mapping	-	ARP protocol Addresses mapping	-	ARP protocol	-	-
LLDP configuration	-	lldp command	-	lldp command	-	lldp command	-	-

SNMP configuration	SNMP menu	SNMP daemon	SNMP menu	SNMP daemon	SNMP section	SNMP daemon	SNMP settings	SNMP settings
MINT configuration	Link Settings	mint command (MINT version) mint command (TDMA version)	Link Settings	mint command (TDMA version)	-	-	-	-

Infrastructure

The infrastructure security is an important aspect concerning the information security, which requires special attention. The infrastructure implementation depends on the technical policy of the enterprise. The network should have functionalities such as logging, monitoring and technical record-keeping.

Monitoring

A monitoring system is required for centralized device management and network operation monitoring. Also, the monitoring system sends notifications to engineers if the parameter values are outside the allowed range. Such notifications reduce the service personnel response time, thereby minimize the consequences of failures and possible attacks.

Monitoring systems can be integrated with alarm systems and video surveillance.

Infinet provides its own system for monitoring the Infinet wireless devices - InfiMONITOR. The monitoring system collects data in the following ways (Figure 16):

- **Polling:** the monitoring system sends SNMP requests to the devices, demanding specific parameters. The device generates an SNMP response for the monitoring system, where it indicates the values of the requested parameters. The device parameter polling is carried out with a set periodicity, which guarantees that each device will be interrogated in a given interval.
- **Traps:** the device sends a special SNMP Trap message to the monitoring server in case of an incident from the specified list. The SNMP Trap sending is initiated by the device itself and occurs instantly, regardless of the polling cycle, however, this will require additional device configuration.

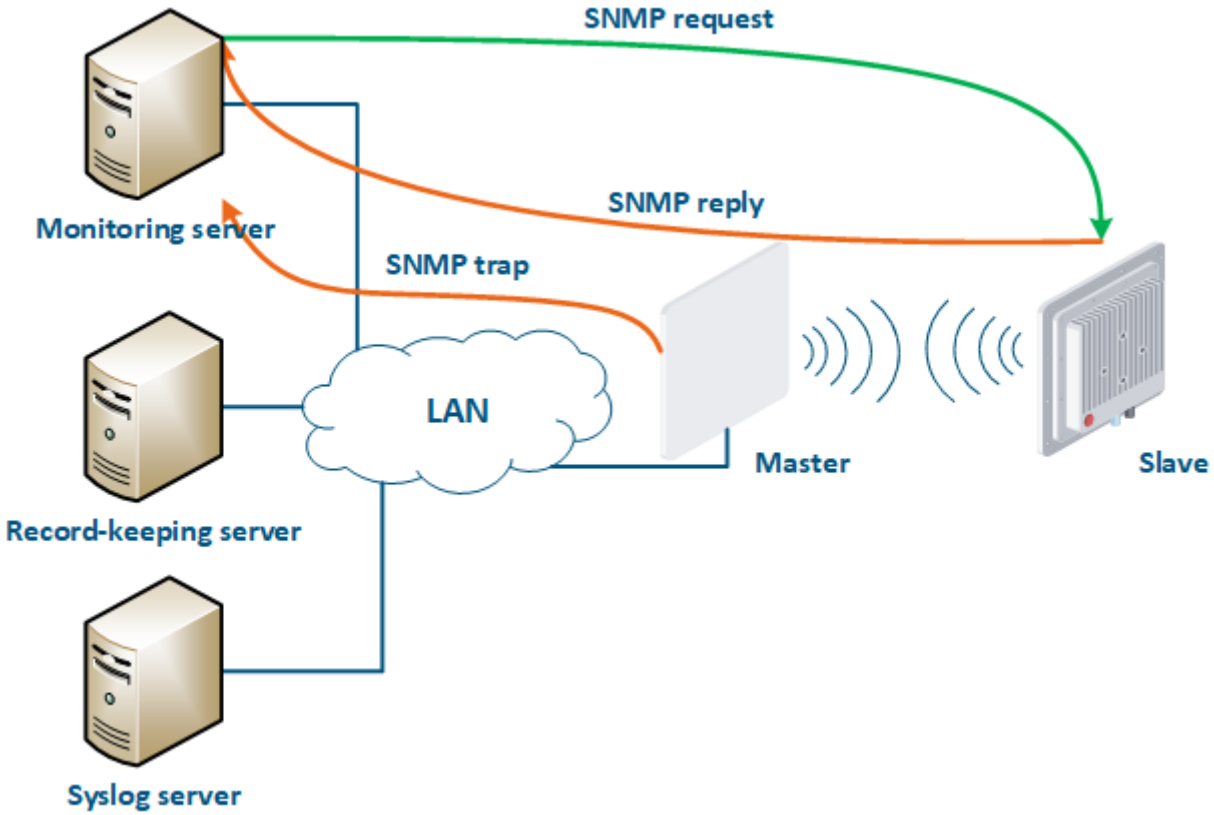

Figure 16 - Data exchange between devices and a monitoring system

Syslog storage

A detailed incident investigation requires an analysis of the system logs stored on the device. Infinet devices support logging, but the system log will be lost after a device reboot. In large networks it is useful to have a centralized repository of log files. Such a repository has an interface which allows to display all the network's devices logs necessary for the incident investigation.

A Syslog server is allocated on the network for these purposes. All log entries are sent to the Syslog server simultaneously with writing to the system log (Figure 17). This allows to centrally store the message history of all the network devices, without the risk of losing all syslog data in case of device reboot or unauthorized access.

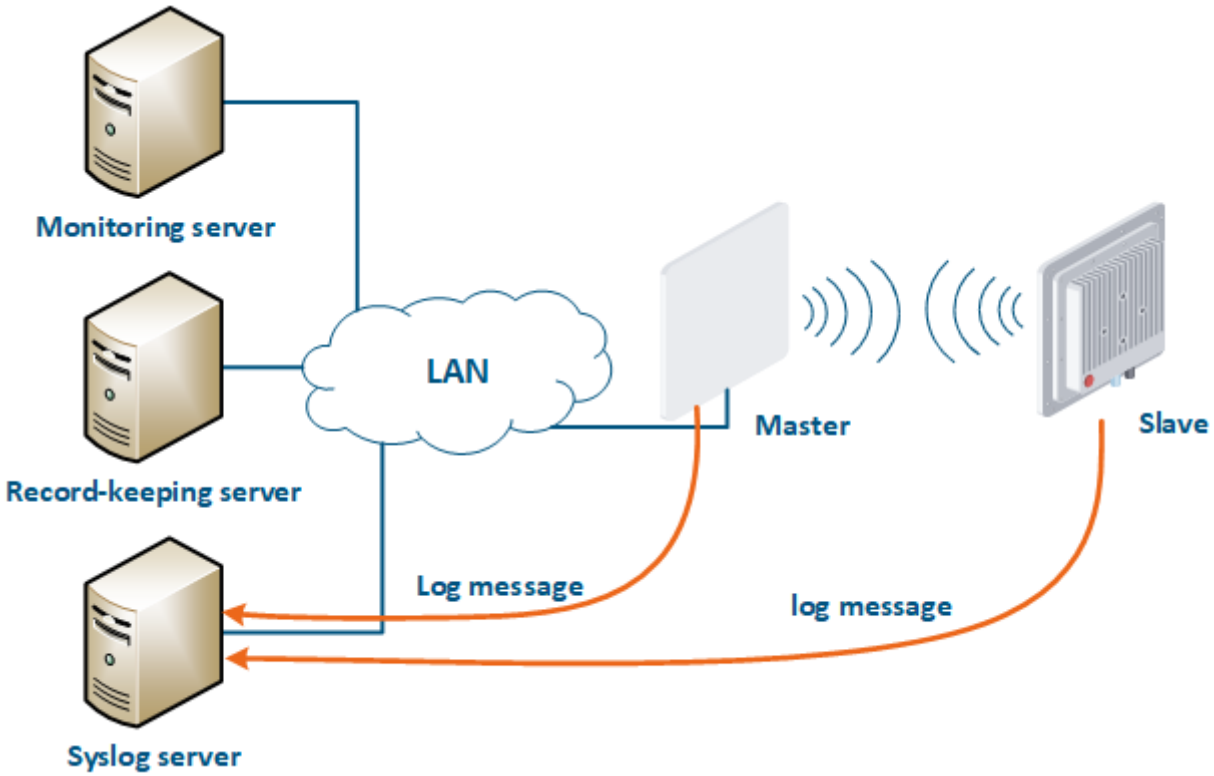

Figure 17 - Data exchange with the Syslog server

Technical record-keeping

Operational problems solving, to gain access to the facility, to restore the configuration and add it to the monitoring system, etc requires a comprehensive information about the devices. Such information includes both technical and administrative aspects. Special technical record-keeping systems can be used on the network to store the data and have access to it. Technical record-keeping systems contain the following information:

- **Device info:** indicates the device model, its serial number and network details.
- **Site info:** indicates the device location, information about access to the site, contact information, etc.
- **Text device configuration:** The device's configuration history can be used during incident investigation and for device operation restoring, therefore, configuration backups should be performed regularly. Some technical record-keeping systems can be joined with systems of mass devices configuration on the network: such systems allow to unify the configuration of the devices and the network is seen as a single device for which the history of changes is stored.

Infrastructure security measures implementation for devices families

Infrastructure security measures

Measures	InfiLINK 2x2 / InfiMAN 2x2		InfiLINK Evolution / InfiMAN Evolution		InfiLINK XG / InfiLINK XG 1000		Quanta 5 / Quanta 6	Quanta 70
	Web	CLI	Web	CLI	Web	CLI	Web	Web
InfiMONITOR monitoring system	InfiMONITOR - Technical User Manual							
SNMP configuration	SNMP menu	SNMP daemon	SNMP menu	SNMP daemon	SNMP section	SNMP daemon	SNMP settings	SNMP settings
Traps configuration	SNMP menu	SNMP traps	SNMP menu	SNMP traps	SNMP	SNMP traps	-	

					section			
Syslog display	Device Status menu	General Purpose Command Set	Device Status	General Purpose Command Set	Maintenance	General Purpose Command Set	Maintenance	Maintenance
Incident history sending to a syslog server	-	General Purpose Command Set	-	General Purpose Command Set	-	General Purpose Command Set	General settings	-
Text configuration management	Maintenance menu Command Line menu	General Purpose Command Set	Maintenance menu Command Line menu	General Purpose Command Set	Maintenance	General Purpose Command Set	Maintenance	Maintenance

Additional materials

Online courses

1. InfiLINK 2x2 / InfiMAN 2x2: Initial Link Configuration and Installation.
2. InfiLINK XG Family Product.
3. Quanta 5 / Quanta 6: Installation and Configuration.
4. Wireless Networking Fundamentals.
5. InfiLINK 2x2 and InfiMAN 2x2: Switching.

White papers

1. Link aggregation, balancing and redundancy.
2. Connectivity with mobile objects.
3. Dynamic Frequency Selection.

Webinars

1. InfiNet Wireless equipment installation, grounding and lightning protection.
2. Switching configuration using InfiNet Wireless devices - typical scenarios.
3. Link diagnostics for the InfiLINK 2x2 and InfiMAN 2x2 product families.
4. InfiNet Wireless solutions for mobile projects.

Screencast

1. InfiNet Wireless Equipment - From Planning to Commissioning.
2. ERConsole.

Other

1. Acessories section on the infinetwireless.com
2. FTP Infinet Wireless
3. InfiMONITOR section on the infinetwireless.com