10.8. Network Design, Architecture and IP Address Management

Objective

10.8.1. IP Address architecture, allocation and addressing schemes enable and support system security and data protection.

Context

Scope

10.8.2. This section includes discussion of the principles of separation and segregation as network design and network architecture characteristics. It also discusses how IP addresses can be used to support these principles for improved security of larger or multi-classification agency systems.

Background

10.8.3. The larger the network, the more difficult it is to protect. A large, unsegmented network presents a large attack surface with greater susceptibility to the rapid spread and dissemination of system faults, weaknesses, vulnerabilities and attacks. In a non-segmented network, traffic and applications generally have access to the entire network. If a fault occurs or an attacker gains entry, the fault or attacker can move laterally through the network causing disruption, network outages and enabling access to critical operational or classified data.

10.8.4. A large network is also more difficult to monitor and control. Segmenting the network limits an attacker's ability to move through the network by preventing lateral movement between zones. Segmentation also enhances the ability to detect, monitor, control, isolate and correct faults.

10.8.5. A fundamental construct in the management of risk in networks is that of Trust Zones and Trust Boundaries. A Trust Zone is a zoning construct based on levels of trust, classification, information asset value and essential information security. A Trust Boundary is the interface between two or more Trust Zones. Trust Zones use the principles of separation and segregation to manage sensitive information assets and ensure security policies are consistently applied to all assets in a particular Trust Zone. Refer also to Section 22.1 – Cloud Computing and Section 22.2 – Virtualisation.

Separation and Segregation

10.8.6. Separation and Segregation are determined by system function and the sensitivity of the data the system stores, processes and transmits. One common example is placing systems that require a connection to the Internet into a demilitarized zone (DMZ) that is separated and segregated (isolated) from more sensitive systems. Another example is the use of compartments.

10.8.7. Separation and Segregation limits the ability of an intruder to exploit a vulnerability with the intent of elevating privileges to gain access to more sensitive systems on the internal network. VLANs may be used to further separate systems by controlling access and providing segregation thus giving additional protection.

10.8.8. Network segmentation is an effective strategy for protecting access to key data assets, and impeding the lateral movement of system faults, threats and malicious activity. Segregation has the following benefits:

- Enhanced performance: with fewer hosts per subnet, there is a reduced signalling and traffic overhead allowing more bandwidth for data communication.
- Improved security: with less signalling traffic going through all network segments, it is more difficult for an attacker to analyse the addressing scheme and network structure. Failures in one segment are less likely to propagate and more robust access control can be established and enforced.

10.8.9. Effective segregation also requires:

- Specialised knowledge: networks may support many devices with complex policies and rule sets. Support staff must be properly educated and trained to ensure the network segmentation is maintained.
- Administrative effort: changes in infrastructure, such as new applications and new technologies, can extend the time required to make changes and ensure the integrity of network segments.
- Infrastructure Investment: segregation may require more equipment, new equipment with advanced functionalities, or specific software to deal with multiple segments. These requirements should be considered during budget planning.

ISO 27001 and ISO 27002 implementation recommendations for network segregation

10.8.10.

These ISO Standards require the implementation of network segregation. In particular they recommend that groups of information services, users, and information systems are segregated on networks. Specific recommendations are summarised below:

- Divide large networks into separate network domains (segments);
- Consider physical and logical segregation;
- Define domain perimeters;
- Define traffic rules between domains;
- Use authentication, encryption, and user-level network access control technologies;
- Consider integration of the organisation's network and segments with those of business partners.

10.8.11. The following structures and techniques should be considered:

- **Criteria-based segmentation**: Pre-define rules to establish perimeters and create new segments in order to reduce unnecessary redesign and future administrative overheads. Examples of criteria are trust level (e.g., external public segment, staff segment, server segment, database segment, suppliers segment, etc.), organisational unit (e.g., Operations, Service Desk, Outreach, etc.), and combinations (e.g., external public access).
- **Use of physical and logical segmentation:** Depending upon the risk level identified in the risk assessment, it may be necessary to use physically separated infrastructures to protect the organisation's information and assets (e.g., classified data flowing through a dedicated fibre), or you may use solutions based on logical segmentation like Virtual Private Network (VPN).
- **Access rules for traffic flowing**: Traffic between segments, including those of permitted external parties, should be controlled according to the need to access information. Gateways should be configured based on information classification and risk assessment. A specific case of access control applies to wireless networks, since they have poor perimeter definition. The recommendation is to treat wireless communication as an external connection until the traffic can reach a proper wired gateway before granting access to internal network segments. Refer also to Chapter 19 – Gateway Security.

Network Design

10.8.12 A poorly designed network has increased support costs, reduced availability, security risks, and limited support for new applications and solutions. Less-than-optimal performance affects end users and access to central resources. Some of the issues that stem from a poorly designed network may include the following:

- **Failure domains**: One of the most important reasons to implement an effective network design is to minimise the spread and extent of faults. When Layer 2 and Layer 3 boundaries are not clearly defined, failure in one network area can have a far-reaching effect.
- **Broadcast domains**: Broadcasts exist in every network. Many applications and network operations require broadcasts to function correctly; therefore, it is not possible to eliminate them completely. In the same way that avoiding failure domains involves clearly defining boundaries, broadcast domains should have clear boundaries and include an optimal number of devices to minimise the negative impact of broadcasts.
- **MAC unicast flooding**: Some switches limit unicast frame forwarding to ports that are associated with the specific unicast address. However, when frames arrive at a destination MAC address that is not recorded in the MAC table, they are flooded out of the switch ports in the same VLAN except for the port that received the frame. This behaviour is called unknown MAC unicast flooding.
- Because this type of flooding causes excessive traffic on all the switch ports, network interface cards (NIC) must contend with a larger number of frames on the wire. When data is propagated on a connection or network segment for which it was not intended, security can be compromised.
- **Multicast traffic on ports where it is not intended**: IP multicast is a technique that allows IP traffic to be propagated from one source to a multicast group that is identified by a single IP and MAC destination-group address pair. Similar to unicast flooding and broadcasting, multicast frames are flooded out all the switch ports. A robust design allows for the containment of multicast frames while allowing them to be functional.
- **Difficulty in management and support**: Traffic flows can be difficult to identify in a poorly designed network. This can make support, maintenance, and problem resolution time-consuming and difficult as well as creating security risks.
- **Possible security vulnerabilities**: A switched network that has been designed with little attention to security requirements at the access layer can compromise the integrity of the entire network.
- **Criteria-based segmentation**: Pre-define rules to establish perimeters and create new segments in order to reduce unnecessary redesign and future administrative overheads. Examples of criteria are trust level (e.g., external public segment, staff segment, server segment, database segment, suppliers segment, etc.), organisational unit (e.g., Operations, Service Desk, Outreach, etc.), and combinations (e.g., external public access).

Design Implementation

10.8.13. To assist in the implementation of separation and segregation as network design and architectural principles, the following aspects should be considered:

- Classification;
- Security Zones;
- IP Address Management;
- Central Information Repository;
- Private Use of Reserved Addresses;
- Devices with Default IP Addresses; and
- Connector types and cable colours.

Classification

10.8.14. Classified systems should, by definition, be segregated. This is particularly important where network elements have access to compartments and

compartmented data.

10.8.15. Ideally compartmented elements of systems should be segregated and separated from the main network. This may include the use of a reserved address space, monitored to detect violations or unauthorised attempts to connect to compartments or to access compartmented data.

Security Zones

10.8.16. A security zone is a group of one or more physical or virtual firewall interfaces and the network segments connected to the zone's interfaces. Protection for each zone is individually specified and controlled so that each zone receives the specific protections it requires according to classification, endorsement, compartment and sensitivity of data.

IP Address Management

10.8.17. The fundamental goal of an IP addressing scheme is to ensure network devices are uniquely addressed. IP Address Schemes are a fundamental part of any network's security architecture and should support network separation and segregation. There are a number of techniques to assist in separating and segregating network elements. It is also useful to consider how to segregate and control network traffic through:

- Defined network perimeters and boundaries; and
- Defined network traffic rules.

10.8.18. A well-structured IP addressing scheme promotes the ability to quickly identify node properties from an IP address which assist in network management and fault finding and rectification.

Address Block Allocation

10.8.19. There are two main difficulties when assigning address blocks for types of devices. First is that over time there is insufficient provision for additional devices and network growth. When the allocated address block is exhausted, the addressing scheme is compromised (broken). The second is that you have a small number of devices in an address block, but are running out of addresses in other parts of the network. If you "borrow" from a pre-assigned address range, the addressing scheme is also compromised.

10.8.20. Internal IP address ranges are defined by the IETF. Commonly known as RFC 1918 addresses, the most recent RFC is 6761. These RFC's define private IP address ranges which cannot be used for external (Internet) IP addressing. Three address ranges (blocks) are defined:

IPv4 Address Range	Network IPv4 address Block	Directed Broadcast IPv4 address	IPv4 Addresses
10.0.0.0 to 10.255.255.255	10.0.0.0/8	10.255.255.255	16,777,216
172.16.0.0 to 172.31.255.255	172.16.0.0/12	172.31.255.255	1,048,576
192.168.0.0 to 192.168.255.255	192.168.0.0/16	192.168.255.255	65,536

10.8.21. IPv4 addresses are 32-bit binary addresses, divided into 4-Octets and normally represented in a decimal format. An example of IPv4 address is 192.168.100.10. IPv6 addresses are so much larger than IPv4 addresses and impractical to clearly represent in decimals. IPv6 addresses are usually represented in hexadecimal numbers, separated by a colon. An example of an IPv6 address is 2001:0DB8:0000:0002:0022:2217:FF3B:118C. Private IPv6 addresses are specified in RFC 4193

10.8.22. Private addressing is a means of distinguishing networks, assisting in separation and segregation.

Private use of reserved addresses

10.8.23. Some IP addresses have been reserved in IETF standards. Despite official warnings, some organisations use parts of the reserved IP address space for their internal networks where address space is exhausted or poorly designed. This creates conflicts with devices and signalling traffic protocols which can create network faults, anomalies and network outages. This practice is strongly discouraged.

Devices which have default IP addresses

10.8.24. Some devices are supplied with default IP addresses. If using the IETF RFC 1918 addressing protocol (e.g. 10.0.x.x) some devices may have been allocated the same (duplicate) IP address.

10.8.25. It is important to change default addresses to new addresses that conform with the addressing scheme selected for the agency.

DHCP

10.8.26. In theory, there is only one network device that absolutely needs a true static address, the DHCP server. In practice, it is preferable to assign address blocks to major groups of devices for control, fault isolation and security purposes. Traditionally static devices are provided with a reserved

address. These devices may include:

- DCHP Server;
- Gateway devices;
- Firewalls;
- Routers; and
- Switches.

10.8.27. The majority of other devices can be allocated a DHCP address.

10.8.28. It is important to identify the essential device groups using a risk assessment, operational characteristics, level of security, system classification and other relevant architectural features, business requirements and operational constraints.

Connector Types and Cable Colours

10.8.29. Cable management is discussed in detail earlier in this chapter. In particular note the discussion (10.1.4) of Red/Black concepts which includes separation of electrical and electronic circuits, devices, equipment cables, connectors and systems that transmit store or process national security information (Red) from non-national security information (Black)

10.8.30. Wherever practical and possible, connectors for systems of different classifications should be distinct and be selected to avoid accidental cross-connection of systems of different classifications. This can be achieved through the use of colour and keyed connectors where the colour and keying is different for each classification level or compartment (refer also to 10.1.30 and 10.6.6).

Central Information Repository

10.8.31. Creating a central repository of all the information on networks, IP addresses and devices, is critical to maintaining control of the network. The challenge with traditional tools is that there are often specific tools for each category of devices: one system to track virtual machines, one system to track wireless users, one system to track Windows servers, one system to track Linux machines, etc.

10.8.32. A single repository where all the data relevant to networks, hosts, servers, dynamic clients, and virtual environments can be tracked and synchronised is essential for larger networks. The ability to search across all this information will enable network teams to quickly track changing network landscapes and rapidly troubleshoot issues as they arise. In addition, business data related to a network resource helps bind together the logical network construct and the reality of IT resources.

References

10.8.33. Further references can be found at:

Reference	Title	Publisher	Source
	Network Segmentation and Segregation	ASD	Implementing Network Segmentation and Segregation | Cyber.gov.au
	Cisco on Cisco Best Practices – Cisco IP Addressing Policy	Cisco	Cisco IT IP Addressing Best Practices
	IP Addressing and Subnetting for New Users, Document ID: 13788	Cisco	Configure IP Addresses and Unique Subnets for New Users (cisco.com)
	IP Addressing: IPv4 Addressing Configuration Guide, Cisco IOS Release 15S	Cisco	IP Addressing: IPv4 Addressing Configuration Guide, Cisco IOS Release 15S - Cisco
	Introduction to Server and Domain Isolation	Microsoft	Introduction to Server and Domain Isolation | Microsoft Learn
ISO/IEC 27001:2013	**Information technology -- Security techniques -- Information security management systems -- Requirements**	ISO	https://www.iso.org/standard/54534.html
ISO/IEC 27002:2022	**Information security, cybersecurity and privacy protection — Information security controls**	ISO	https://www.iso.org/standard/75652.html
RFC 1518	**An Architecture for IP Address Allocation with CIDR**	IETF	https://datatracker.ietf.org/doc/html/rfc1518
RFC 1918	**Address Allocation for Private Internets**	IETF	https://datatracker.ietf.org/doc/html/rfc1918
RFC 2036	**Observations on the use of Components of the Class A Address Space within the Internet**	IETF	https://datatracker.ietf.org/doc/html/rfc2036
RFC 2050	**Internet Registry IP Allocation Guidelines**	IETF	https://datatracker.ietf.org/doc/html/rfc2050
RFC 2101	**IPv4 Address Behaviour Today**	IETF	https://datatracker.ietf.org/doc/html/rfc2101
RFC 2401	**Security Architecture for the Internet Protocol**	IETF	https://datatracker.ietf.org/doc/html/rfc2401
RFC 2663	**IP Network Address Translator (NAT) Terminology and Considerations**	IETF	https://datatracker.ietf.org/doc/html/rfc2663
RFC 2894	**Router Renumbering for IPv6**	IETF	https://datatracker.ietf.org/doc/html/rfc2894
RFC 3022	**Traditional IP Network Address Translator (Traditional NAT)**	IETF	https://datatracker.ietf.org/doc/html/rfc3022
RFC 3053	**IPv6 Tunnel Broker**	IETF	https://datatracker.ietf.org/doc/html/rfc3053
RFC 3056	**Connection of IPv6 Domains via IPv4 Clouds**	IETF	https://datatracker.ietf.org/doc/html/rfc3056
RFC 3232	**Assigned Numbers**	IETF	https://datatracker.ietf.org/doc/html/rfc3232
RFC 3260	**New Terminology and Clarifications for Diffserv**	IETF	https://datatracker.ietf.org/doc/html/rfc3260
RFC 3330	**Special-Use IPv4 Addresses" (superseded)**	IETF	https://datatracker.ietf.org/doc/html/rfc3330
RFC 3879	**Deprecating Site Local Addresses**	IETF	https://datatracker.ietf.org/doc/html/rfc3879

RFC 3927	**Dynamic Configuration of IPv4 Link-Local Addresses**	IETF	https://datatracker.ietf.org/doc/html/rfc3927
RFC 3956	**Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address**	IETF	https://datatracker.ietf.org/doc/html/rfc3956
RFC 4193	**Unique Local IPv6 Unicast Addresses**	IETF	https://datatracker.ietf.org/doc/html/rfc4193
RFC 4632	**Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan**	IETF	https://datatracker.ietf.org/doc/html/rfc4632
RFC 5214	**Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)**	IETF	https://datatracker.ietf.org/doc/html/rfc5214
RFC 5737	**IPv4 Address Blocks Reserved for Documentation**	IETF	https://datatracker.ietf.org/doc/html/rfc5737
RFC 6040	**Tunnelling of Explicit Congestion Notification**	IETF	https://datatracker.ietf.org/doc/html/rfc6040
RFC 6052	**IPv6 Addressing of IPv4/IPv6 Translators**	IETF	https://datatracker.ietf.org/doc/html/rfc6052
RFC 6081	**Teredo Extensions**	IETF	https://datatracker.ietf.org/doc/html/rfc6081
RFC 6434	**IPv6 Node Requirements**	IETF	https://datatracker.ietf.org/doc/html/rfc6434
RFC 6598	**Reserved IPv4 Prefix for Shared Address Space**	IETF	https://datatracker.ietf.org/doc/html/rfc6598
RFC 6761	**Special-Use Domain Names**	IETF	https://datatracker.ietf.org/doc/html/rfc6761
RFC 6890	**Special-Purpose IP Address Registries**	IETF	https://datatracker.ietf.org/doc/html/rfc6890
RFC 7371	**Updates to the IPv6 Multicast Addressing Architecture**	IETF	https://datatracker.ietf.org/doc/html/rfc7371
RFC 7619	**The NULL Authentication Method in the Internet Key Exchange Protocol Version 2 (IKEv2)**	IETF	https://datatracker.ietf.org/doc/html/rfc7619
RFC 8012	**Label Switched Path (LSP) and Pseudowire (PW) Ping/Trace over MPLS Networks Using Entropy Labels (ELs)**	IETF	https://datatracker.ietf.org/doc/html/rfc8012
RFC 8190	**Updates to the Special-Purpose IP Address Registries**	IETF	https://datatracker.ietf.org/doc/html/rfc8190

Rationale & Controls

Risk Assessment

10.8.34.R.01. **Rationale**

A risk assessment is a fundamental tool in the architecture and design of a network.

10.8.34.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:5815]

Agencies MUST conduct and document a risk assessment before creating an architecture, and designing an agency network.

10.8.34.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:5816]

The principles of separation and segregation as well as the system classification MUST be incorporated into the risk assessment.

Security Architecture

10.8.35.R.01. **Rationale**

It is important that the principles of separation and segregation as well as the system classification are incorporated into the overall security architecture to maximise design and operational efficiency and to provide and support essential security to the network design.

10.8.35.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:5820]

Security architectures MUST apply the principles of separation and segregation.

Identification of major classifications/categories of network segments

10.8.36.R.01. **Rationale**

Identified in the risk assessment, it is essential that the classification of systems is clearly identified and is apparent in all architecture and design elements and systems documentation.

10.8.36.R.02. **Rationale**

Clear distinction of networks of different classifications is reinforced through the use of different IP addressing schemes as well as the application of Red/Black, separation and segregation concepts and principles. Refer also to section 10.1 - Cable Management fundamentals.

10.8.36.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:5825]

The classification and other restrictions on the security and control of information MUST be clearly identified for each part of the Agency network.

Visibility

10.8.37.R.01. **Rationale**

Clear identification and visibility of the classifications or category of a network segment is essential in minimising accidental cross-connections, incident management and in limiting the propagation of errors form one segment to others. This also assists in network maintenance and management.

10.8.37.R.02. **Rationale**

Clear visual identification is supported by the use of IP addressing and cable colour schemes as well as the use of different types of cable connectors for different network segments.

10.8.37.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:5843]

Systems of different classifications MUST be visually distinct.

Information Repository

10.8.38.R.01. **Rationale**

Clear documentation and records of changes to the architecture and construct of a network are essential in change management, planning, design of network modifications, incident management and maintenance of a strong security posture.

10.8.38.R.02. **Rationale**

A single repository where all the data relevant to networks, hosts, servers, dynamic clients, and virtual environments can be tracked and synchronised is essential for larger networks. The ability to search across all this information will enable network teams to quickly track changing network landscapes and rapidly troubleshoot issues as they arise.

10.8.38.R.03. **Rationale**

The repository should also contain business data related to a network resource which helps manage necessary changes and upgrades to a network in a fashion that appropriately allocates IT resources and recognises business needs.

10.8.38.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:5831]

An information repository, containing essential network information, change records and business requirements SHOULD be established and maintained.