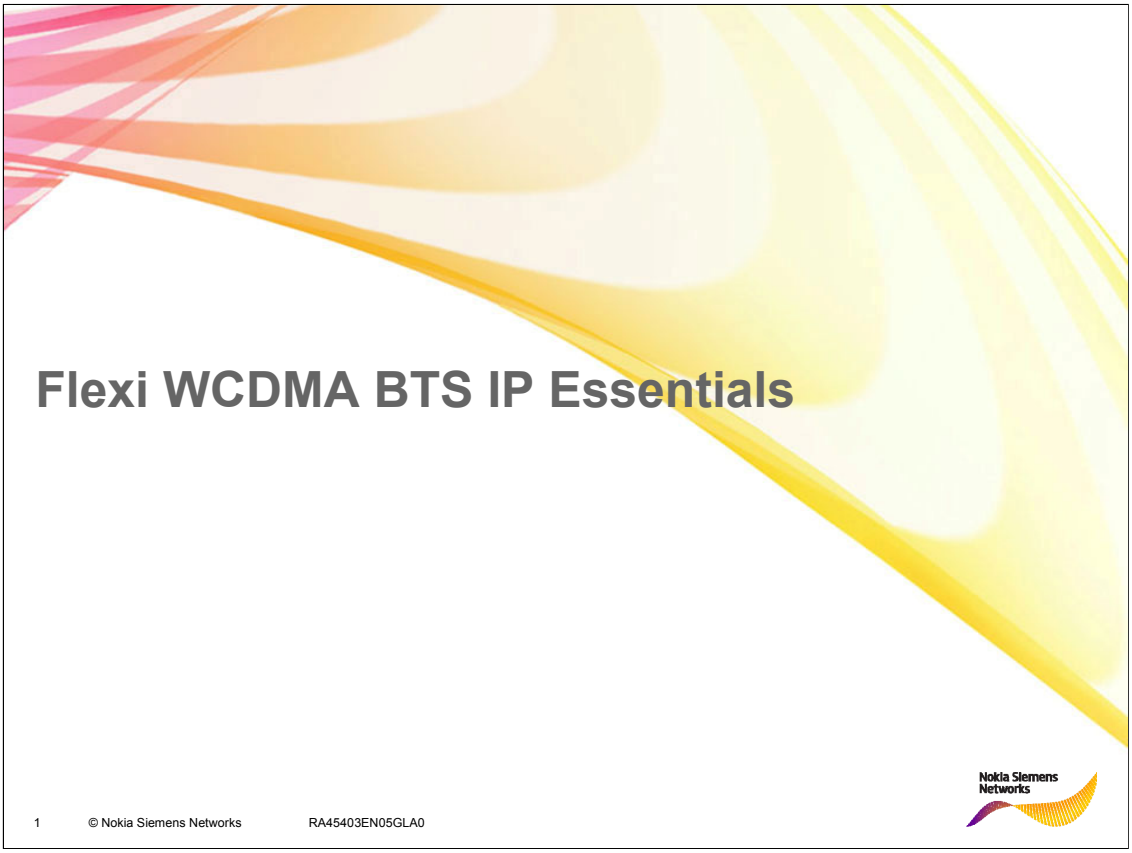

Flexi WCDMA BTS IP Essentials
1
© Nokia Siemens Networks
RA45403EN05GLA0

Nokia Siemens Networks Academy

Legal notice

Intellectual Property Rights

Learning Element Objectives

After completing this Learning Element, the participant should be able to:

- Understand the use of IP SubNet Masking in Nokia Siemens Networks RAS
- Explain the different uses of IP in Nokia Siemens Networks RAS

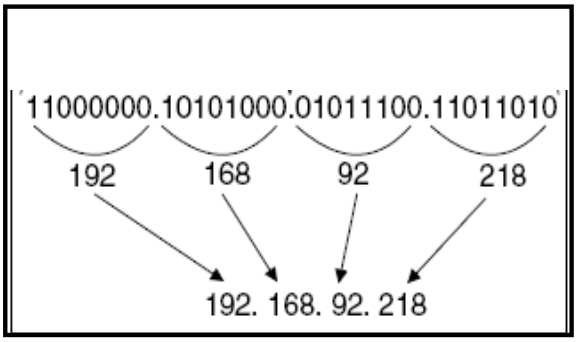
IP Addressing Principles

An IP address is a unique identifier for a host on the Internet. IP addresses are needed for example when information is sent over the Internet.

This Learning Element is divided into following sections:

- IP addresses
- IP subnetting
- Routing

IP Addresses



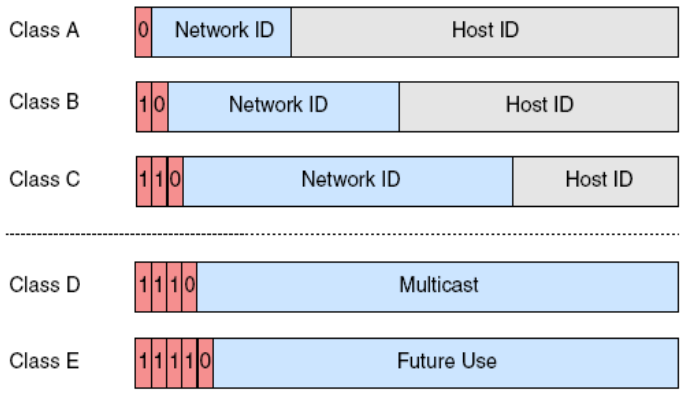
IP version 4 address

Before sending, the data is first broken up into packets. Each of these packets includes a header which indicates the point from which the data originates (source address) and the point to which it is being sent (destination address).

TCP/IP networks use a 32-bit address broken into four 8-bit divisions, called octets. To make the 32-bit address easier to read, IP addresses are usually shown as dotted decimal notations: XXX.XXX.XXX.XXX, where XXX ranges between 0 and 255.

IP addresses consist of a network part and a host part. The structure of the IP version 4 address format is shown in the slide.

IP Address Classes



Assignable IP network addresses fall into five classes: A, B, C, D and E.

Class A network addresses are specified in the first octet.

Class B addresses in the first two octets.

Class C addresses in the first three octets.

The network addresses function like logical area codes for collections of computers. This is often referred to as classful addressing, because each class fixes a boundary between the network-prefix and the host.

The remainder of the IP address identifies the host device address within the network.

Class D addresses are reserved for multicasting and class E addresses for future use.

IP Subnetting

IP address:

192.168.92.218 = 11000000.10101000.01011100.11011010

SubnetMask:

255.255.255.248 = 11111111.11111111.11111111.11111000

Network Address:

192.168.92.216 = 11000000.10101000.01011100.11011000

Example of logical ANDing

For each column, where there is a 1 in the IP address AND in the subnet mask, there is a 1 in the network address; otherwise, there is a zero in the network address

A, B and C class networks can be divided into smaller portions, called subnets. In this case, the IP address consists of three parts: network-prefix, subnet number and host number.

The variable length subnetting prevents network address exhaustion by increasing the number of possible subnetworks.

In order for computers and other network devices to be able to determine which portion of an IP address identifies a network and which identifies a host, subnet masks are needed.

A subnet mask looks like an IP address, but instead, it is used to mask the host portion of an IP address, leaving only the network portion "visible".

Determining the subnet is accomplished through a process called "Logical ANDing". ANDing is a simple operation. It’s best illustrated by converting all the decimal numbers to binary ones, then lining up a device’s IP address and subnet mask, one directly below the other. The process is shown in the example in the slide.

Routing

- Routing is moving information across an inter-network from the source to its destination
- Along the way, at least one intermediate node is typically encountered
- The decision on the correct route is made in each node based on the IP address of the packet

IP packet delivery procedure

- The IP packet delivery procedure depends on the locations of the sender and the receiver. If they are both located in the same Local Area Network (LAN), there is no need for an IP level routing functionality
- In the same LAN, the packet can be sent directly to the receiver by using the receiver's Ethernet address
- The Address Resolution Protocol (ARP) can be used to resolve the Ethernet (MAC) address of a receiver in the same LAN
- If the source and the destination are located in different LANs, an external routing functionality is needed to transfer IP packets from the sender to the receiver
- That means that the IP packet is sent to the router, which forwards the packet to its correct destination
- The decision on what is the correct destination is based on the information in a routing table
- Each row of the IP routing table contains an entry for each network that is known to the router storing this table. Routing tables are configured either manually by a system administrator or automatically by using a suitable routing protocol

Static Routing

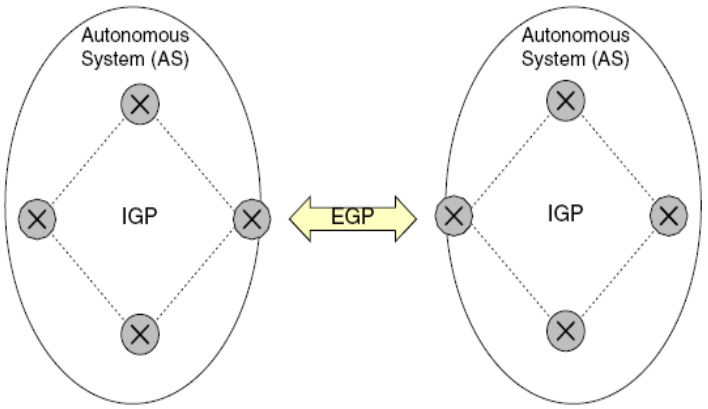
Static routing is performed using a preconfigured routing table. Static routing tables are configured manually, usually by a system administrator.

This is the most basic form of routing, and it usually requires that all devices have static addresses configuration.

An additional requirement is that all the devices stay on their respective networks.

Otherwise, the routing tables have to be altered manually on one or more devices to reflect the change in network topology or addressing.

Dynamic Routing



11 © Nokia Siemens Networks RA45403EN05GLA0

Dynamic routing uses special routing information protocols to automatically update the routing table with routes known by peer routers.

The routing protocol refers to the method used by routers to exchange routing information and forms the basis for providing a connection across an internet.

These protocols are grouped according to whether they are Interior Gateway Protocols (IGPs) or Exterior Gateway Protocols (EGPs).

Interior gateway protocols are used to distribute routing information within an Autonomous System (AS).

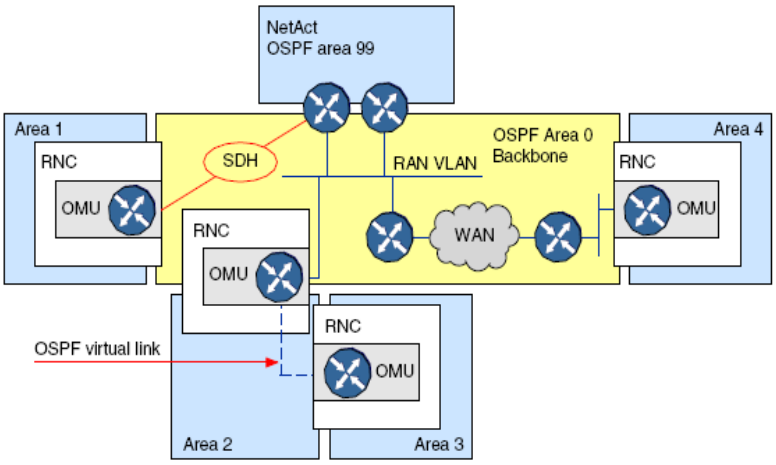
Examples of IGPs are:-

- Open Shortest Path First (OSPF).
- Routing Information Protocol (RIP).

An AS is a set of routers inside the domain administered by one authority.

Exterior gateway protocols, such as Border Gateway Protocol (BGP), are used for inter-AS routing, so that each AS may be aware of how to reach others throughout the Internet.

OSPF Routing



12 © Nokia Siemens Networks RA45403EN05GLA0

OSPF is a link-state routing protocol that sends link-state advertisements (LSAs) to all other routers within the same hierarchical area.

OSPF LSAs include information on attached interfaces, metrics used, and other variables. As OSPF routers accumulate link-state information, they use the SPF (Shortest Path First) algorithm to calculate the shortest path to each node.

Different OSPF Routers

Internal router

Within an area, the functionality of the router is straightforward. It is responsible for maintaining a current and accurate database of every subnet within the area and to forward data to other networks by the shortest path. Flooding of routing updates will be confined to the area.

Backbone router

The design rules for OSPF require that all the areas be connected through a single area known as the *backbone area* or *area 0*. A router within this area is referred to as a *backbone router*. It may also be an internal router or an area router.

Area border router (ABR)

This router is responsible for connecting two or more areas. It will hold a full topological database for each area it is connected to and will send LSA updates between areas. These LSA updates will be summary updates of the subnets within an area. It is as the area border that summarisation should be configured for OSPF, because this is where the LSA's make use of the reduced routing updates to minimise the routing overhead on both the network and the routers.

Autonomous system boundary router (ASBR)

To connect to the outside world, or to any other routing protocol, you need to leave the OSPF domain.

Different Types of Areas

Ordinary or standard area

This area connects to the backbone and it is seen as an entity unto itself. Every router knows about every network in the area and each router has the same topological database.

Stub area

This is an area that will not accept external summary routers. The LSAs blocked are types 3 and 4 (summary link LSAs that are generated by the ABRs). The consequence is that the only way a router within the area can see outside the autonomous system is via the configuration of default route.

Totally stubby area

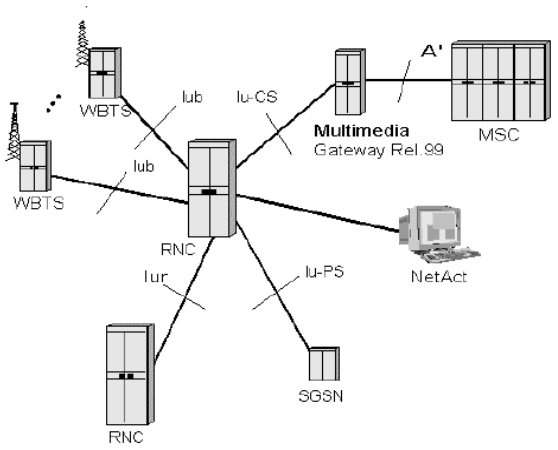
This area does not accept summary LSAs from the other areas or external summary LSAs from outside the autonomous system. The only way out of the area is via a configured default route. This type of area is useful for remote sites that have few networks and limited connectivity with the rest of the network.

Virtual link

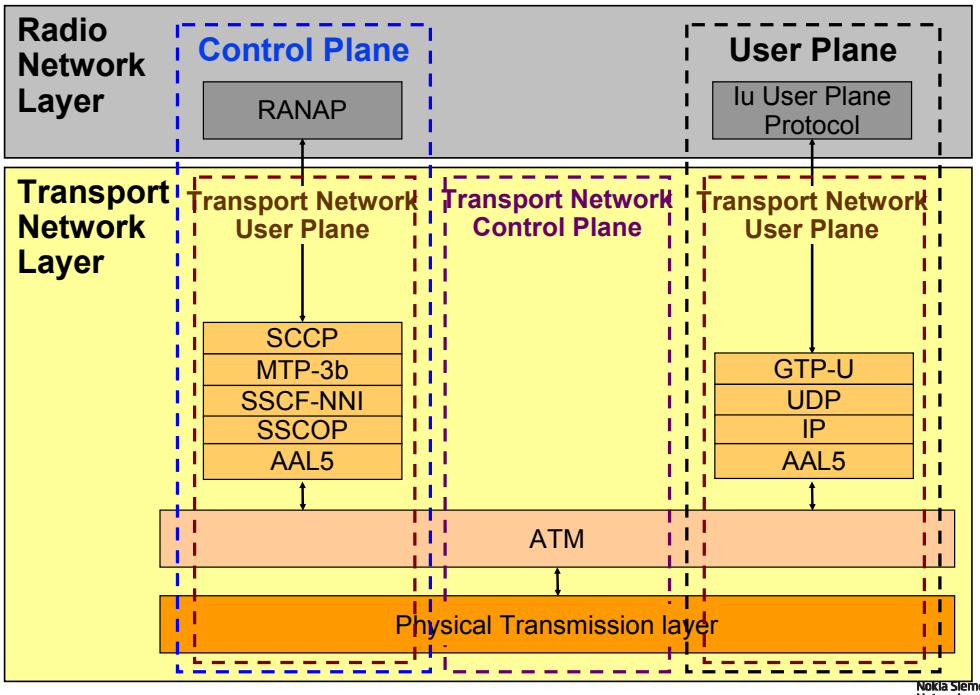
If the new area cannot connect directly to the backbone area, a router is configured to connect to an area that does have direct connectivity.

Iu-PS interface

Iu-PS interface is the interface towards the 3G SGSN from the RNC. The interface uses IP over ATM technology for transporting user data.



Protocol structure for Iu-PS



16 © Nokia Siemens Networks RA45403EN05GLA0

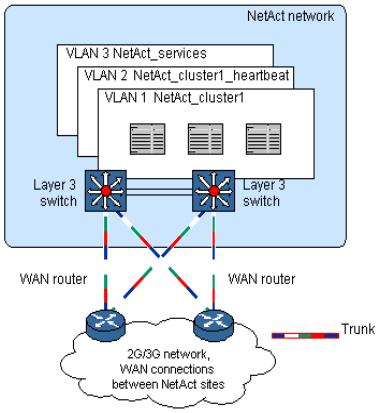
The Transport Network Control Plane is not applied to Iu-PS.
Setting up of GTP tunnel requires only an identifier for the tunnel and the IP addresses for both directions, and these are already included in the RANAP message RAB Assignment.

Data Communication Network (DCN)

The DCN network provides the means of creating an O&M connection between network elements and NetAct as well as between different NetAct sites.

The DCN backbone is the core of the DCN network.

It provides connections to the network elements which are using IP protocol for O&M management, and also to those elements using ISO IP protocol. The DCN backbone also connects different clusters located in different sites.



Data Communication Network (DCN)

DCN architecture of Nokia NetAct consists of the following components

- NetAct DCN backbone
- NetAct office network
- Operator office network

Purpose of DCN network is:

to transfer O&M data between

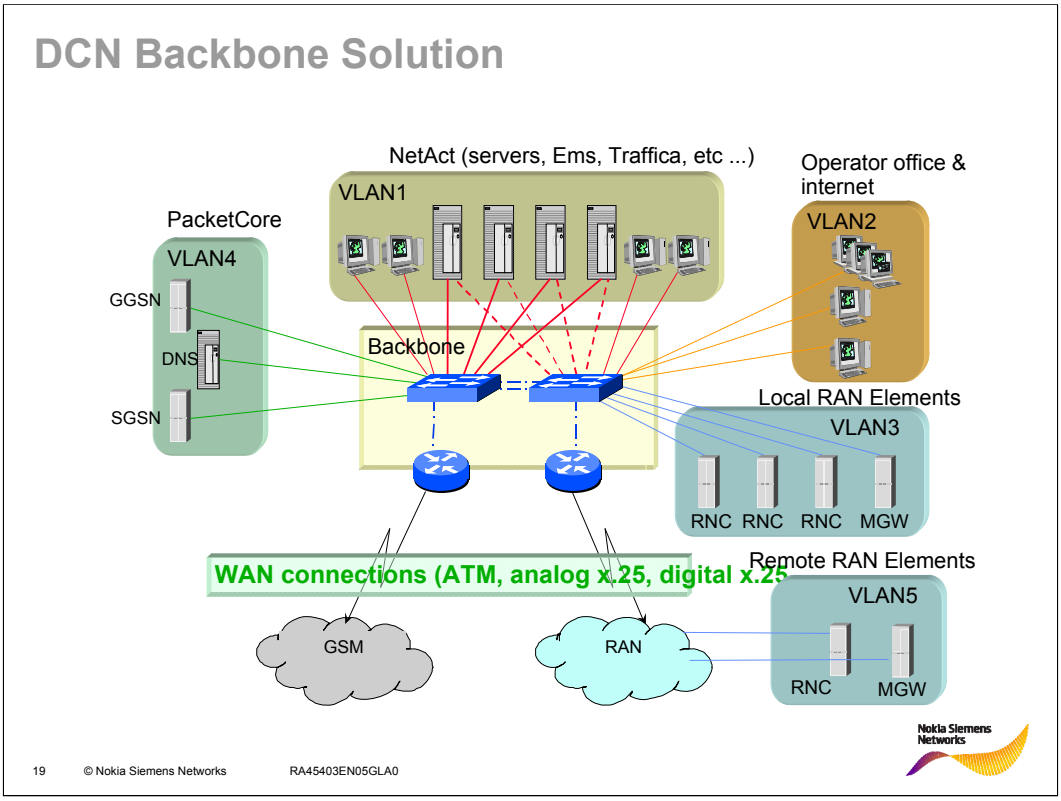
- network element sites
- and different network management sites (regional, global and remote sites)

Key requirements for DCN network are:

- high availability
- security
- standard interface protocols

The following factors affect which DCN solution is available:

- Capacity required
- Cost of equipment and/or leased line
- Current configuration
- Distance between NetAct and its network elements
- Ease of configuration and maintenance
- Quality of service



DCN Backbone solution

The Nokia DCN backbone solutions are designed to be easily modifiable to support management of separate networks.

The core of DCN architecture in each site forms a DCN backbone - redundant and unified solution that can be utilized both in Regional and Global clusters. The DCN backbone also provides the means of interconnection between different clusters located on different sites. It is possible to protect the connections between the clusters with VPNs (Virtual Private Networks).

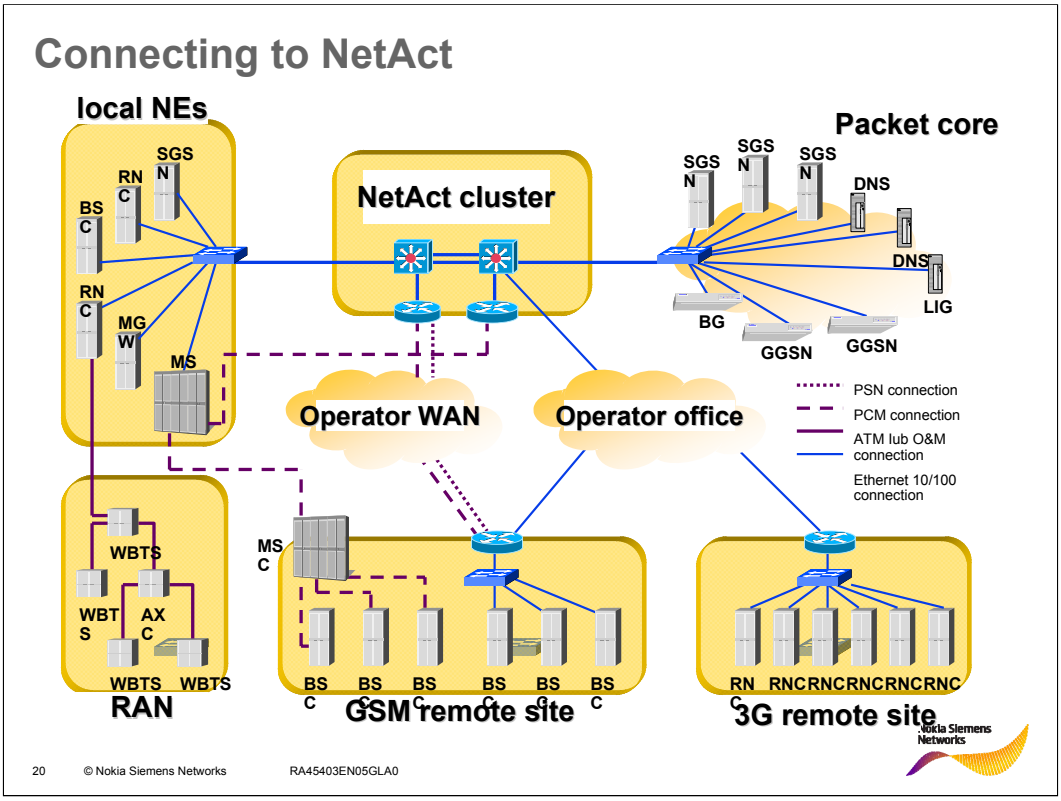
The management interfaces to GSM, packet core and RAN networks are provided by the DCN backbone. Both LAN and WAN connections are supported. Local elements can be connected to the backbone switches, WAN connections are provided by the backbone routers.

VLAN

Different (logical) parts of network are divided into virtual LANs (VLANs), for example to NetAct servers and local network elements. Routers route packets between the VLANs. The NetAct network is divided into several separate VLANS to provide a better structure.

A VLAN group of devices on one or more local area networks that communicate as if they were attached to the same wire, although they are located on a number of different local area network segments

In terms of IP addressing, each VLAN forms one subnet and the size of this IP subnet depends on the number of hosts present in it. When creating the IP subnet it is always recommended that some extra IP addresses are reserved for future expansion.



Network topologies

The procedure for planning a DCN is determined by the network topology used.
In essence, network topologies define the cabling layout of your network. Once the network topology is defined, identify the network services and protocols to be used.
In OSS3.1, it is recommended that the local network elements are connected to NetAct with LAN. For establishing WAN connections there are several possibilities:

- Remote site connections over serial line by using HDLC (Cisco router on both the remote and local site) or PPP
- Tunnelling ISO IP over TCP/IP between the local and remote sites
- ATM (by using IMA) connection to the RAN network elements
- X.25 connection to the GSM network elements (PCM/PSN)

Network interfaces

The interfaces provided by the DCN backbone are listed below.

- LAN interfaces:
  - IEEE802.3 10/100 Mbps
- WAN interfaces:
  - E1
  - ATM - E1 (IMA) 4/8 E1 port
  - Synchronous serial

BTS Site IP Subnet Configuration Example
(Ultrasite WCDMA BTS)