


Application Paper

A Guide to Open Broadband Access with Iskratel's Products



Implementing the Two-Tier Open-Access Model

Tomo Bogataj, Simon Čimžar, April 2009

Contents

1	Summary	2
2	The Big Picture: Principles of Operation	3
2.1	The Two-Tier Open-Access Model	3
2.2	Management Domains	4
2.3	Awareness Domains	5
2.4	Isolation of Customers' Flows	7
2.5	VLAN-per-Service Architecture	8
3	The Necessary Ingredients	8
3.1	Service-Selection Portal	8
3.2	Manageability of the Broadband-Network Termination	10
4	Putting It All Together	11
4.1	Bringing Services to Life	11
4.2	Selecting from among Services	13
5	The Road Ahead	14
5.1	Service Integration and the Integrated Open-Access Model	14
5.2	Efficient and Secure Video Delivery	15
5.3	Extending the Service Provider's Reach	15
5.4	Transparent Management – Gemini is the Future	17
6	Final Thoughts.....	18
7	Abbreviations	19
8	References	19

1 Summary

The open-access model makes possible the free selection of services and providers to broadband-access customers, and at the same time guarantees equal terms to service providers when they are offering their services.

Separation of domains – Efficient delivery of services

The practical implementation of the two-tier open-access model using Iskratel's products introduces a clear separation between the domains of network and service providers: they operate and manage their networks and services within their confined domains. The network provider operates and manages the access and aggregation network, and provides layer-two paths for the services, but remains unaware of higher-layer service-related parameters. The service providers deliver the services to the customers and manage the service-related settings, but need to take no interest in how the service paths are established.

Secure VLAN-per-service architecture – No IP-addressing conflicts

The implementation uses the VLAN-per-service architecture, avoiding service-identification ambiguities that might occur due to IP-addressing conflicts. At the customer premises, individual service VLANs map to physical network ports of the broadband-network termination. Security features on the MSANs prevent direct communication between customers across the access network, assisting in the enforcement of proper service policing and billing, and protecting network resources.

Automated service selection – Bringing infinite choices at low cost

The customers make their freedom of service selection by means of a service-selection portal. They use it to subscribe to new services, cancel existing services, or change service providers. Automated reconfiguration procedures, triggered by the service-selection portal, provide lower operational costs to the providers, while improving customer satisfaction.

2 The Big Picture: Principles of Operation

Open access is an access model that provides broadband-access customers (end users) with fair access to services, provided by different – and usually competing – service providers (SPs). All the service providers share the same network resources and the equipment of a single network provider (NP).

To the customers the open-access model gives a free choice of services and service providers; to individual service providers it guarantees equal terms for offering their services (internet, voice, video, and others) to customers.

The open-access model gives customers freedom of choice with regard to the services they take. While using voice services from one SP, customers may use internet/data services from another SP, video services from yet another SP, and so on. Furthermore, customers may even collect services of the same kind from different SPs. In this way, customers minimize the costs of the services they use and/or improve the quality of their experience.

2.1 The Two-Tier Open-Access Model

This document focuses on the use of the two-tier open-access model, although other open-access models are also feasible (i.e., the three-tier model and the integrated model) [1].

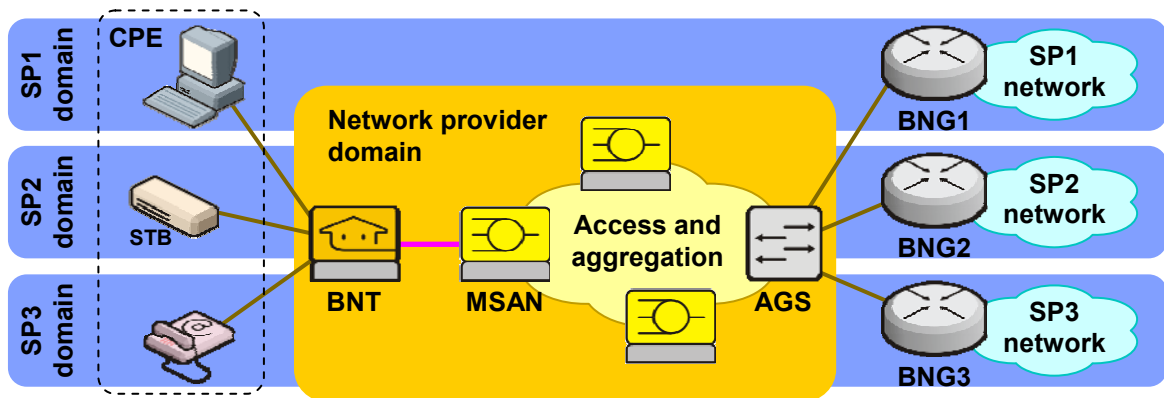


Figure 1: Two-tier open-access model

Within the two-tier open-access model (Figure 1), individual service providers (SPs) only provide their customers with the services they are specialized in. They all maintain their service networks individually, and provide their own broadband-network gateways (BNGs) as the connection points for the services they offer over the NP's network. The network provider's broadband network termination (BNT) and the aggregation switch (AGS) are the points where all the SP's services converge to the NP's transport platform.

In the two-tier model, any customer-premises equipment (CPE) device is owned by the SP that provides the service.

2.2 Management Domains

The NP and all the SPs operate, maintain and manage their networks, equipment and services (Figure 1) within their confined domains. The majority of management flows is intra-domain (within their domains), while some management interactions take place between the domains (Figure 2).

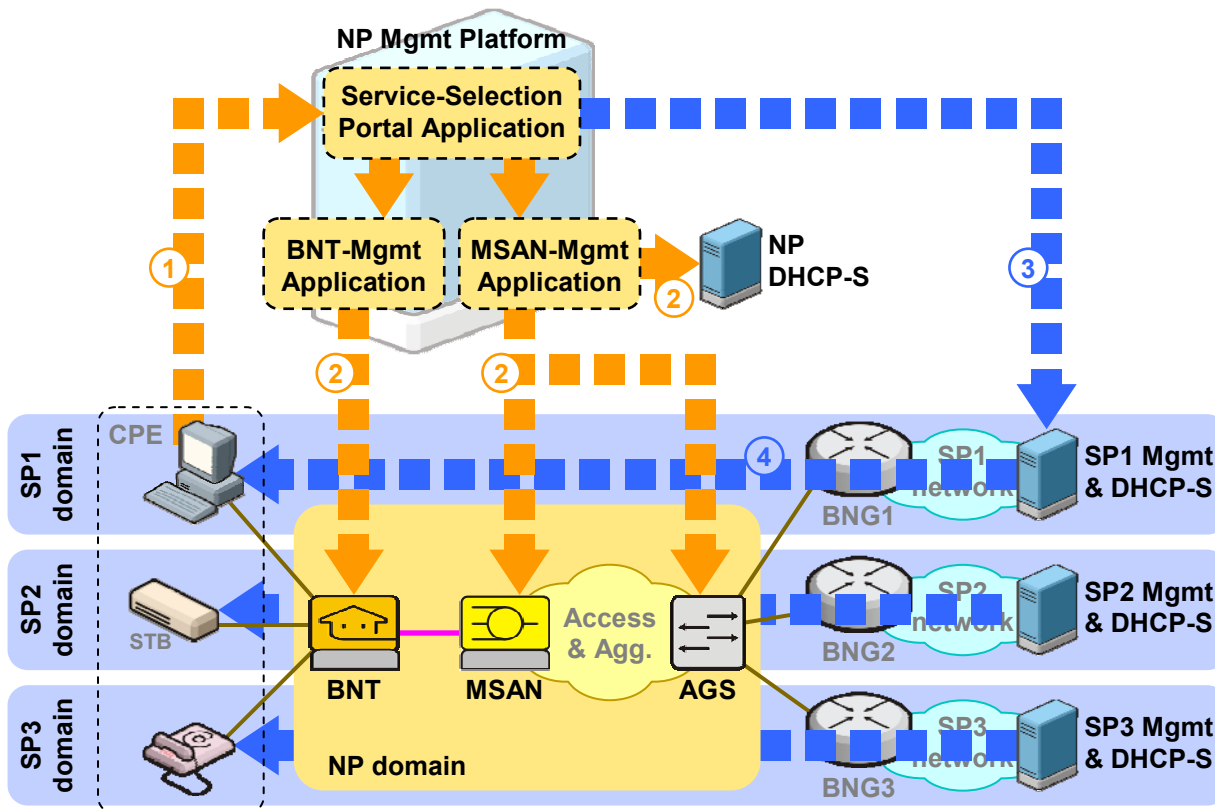


Figure 2: Management domains and flows

The basic principle of management is relatively straightforward. It is composed of four phases: service selection, path provisioning, inter-provider notification, and service provisioning.

1. Service selection

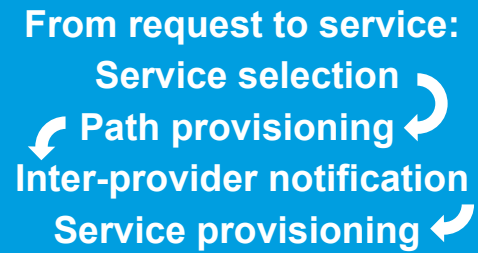
The customer uses the customer-premises equipment (CPE) – a personal computer or a set-top box (STB) – to access the service-selection portal (SSP). At the SSP, the customer selects the services that he or she wishes to use, subscribes to the new services or cancels existing services, or changes the service provider for a given type of service (e.g., internet, voice, or video).

2. Path provisioning

When the customer's choice of services is changed, the SSP triggers the necessary configuration changes across its management domain (the access and aggregation network) in order to set a path for a service between the customer's CPE and the SP's BNG. The SSP does so via the BNT-management and MSAN-management applications on the NP's management platform. To facilitate an automated configuration of the MSAN and the BNT, the management platform also stores the MSAN's and the BNT's new configuration on the NP's dynamic host-configuration protocol (DHCP) server.

3. *Inter-provider notification*

Besides triggering a configuration change across the NP's domain, the SSP also notifies the affected SP (or several SPs) of the changes that the customer made. The SP's management system makes the necessary service-related changes on the SP's BNG and on the SP's DHCP server.



4. *Service provisioning*

Whatever configuration changes are necessary on the CPE, they are all performed within the SP's management domain, between the SP's management & DHCP server and the customer's CPE.

The process of service selection and/or configuration is thus completed: the path for the service is set across the NP's domain, and the service is configured and enabled across the SP's domain, all the way to, and including, the customer's CPE.

Network provider's management platform

The NP's management platform is at the heart of all the management operations. The platform integrates four components:

- the BNT-management application,
- the MSAN-management application,
- the Service-selection portal,
- the DHCP server.

Typically, these are all co-located on a single hardware platform in order to reduce the NP's costs. However, the NP may use independent hardware elements to house individual management applications.

2.3 Awareness Domains

The separation of the responsibilities of the NP, on the one hand, and the SPs, on the other, is clear:

- The NP must provide a path for the services through its network, between the CPE and the BNGs. At the same time, the NP does not need to be aware of the services themselves.
- The SPs must deliver services to the customers, using the NP's network to do this. However, they do not need to care about how the NP provides the connectivity for the services.

What follows from the above observation is the separation of the networking levels that the NP and the SPs need to be aware of:

- The NP uses individual VLANs as "tunnels" across its domain. Each service is assigned a unique VLAN ID in the NP's network. The NP provides the VLAN "tunnels" but does not care about the IP addressing of the IP packets transported through these VLAN "tunnels".
- The SPs use VLAN "tunnels" as a means to deliver the services to the customers. They assign the IP addresses to the CPE to make the delivery possible, but do not care about the assignment of the VLAN IDs within the NP's network.

A clear division between the domains of the NP and the SPs allows them to optimize their operation and management processes.

In addition to the VLAN "tunnels" assigned for the services, the NP also uses an additional VLAN for the management of the BNTs, and since the BNTs are within the NP's domain, the NP also assigns IP addresses to the BNTs for the purposes of management. Figure 3 illustrates the use of VLAN "tunnels" and IP-address assignment to the BNTs and to the CPE.

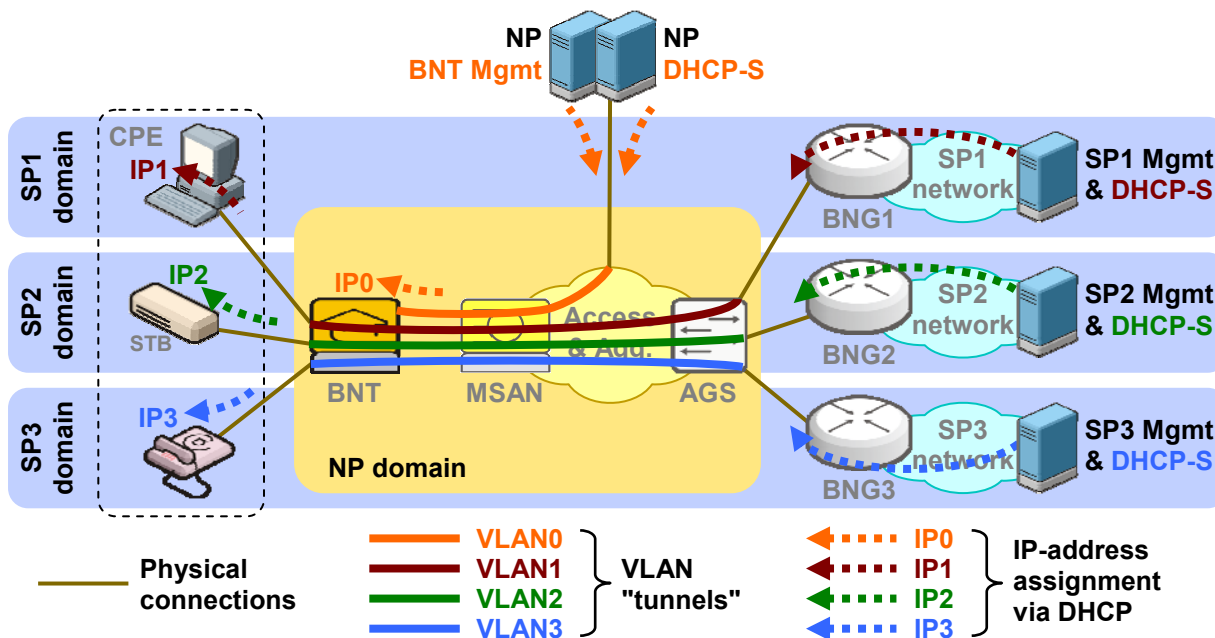


Figure 3: VLAN and IP-address assignment

The model uses the VLAN-per-service architecture for the service delivery to the customers. This means that on each broadband connection between the MSAN and a BNT, the number of unique VLANs equals the number of services that the customer uses, plus one VLAN for the management of the BNT. The BNT-management VLAN aside, the VLANs on each BNT correspond to the services that are used by the customer.

Network provider's domain – VLAN paths through the network

The NP is responsible for the setup and management of the VLANs across its own domain, i.e., on MSANs, on BNTs, and on aggregation switches. At the same time, the elements of the NP's access and aggregation network remain completely unaware of the IP addresses of the SPs and their services, which use the VLAN "tunnels" in the NP's domain.

The NP is aware of and manages the IP addresses of the BNTs at the customers' premises. A DHCP server, which is a part of the NP's management platform, assigns the IP addresses to the BNTs within the BNT-management VLAN. The use of DHCP option 82 (line ID) assists in the identification of the customer, while the use of DHCP option 43 (vendor-specific data) further enables the automated configuration of the BNTs. During runtime, the BNTs are managed via the command-line interface (CLI) or the simple network-management protocol (SNMP).

**The NP manages
VLAN paths across
its domain**

In the spirit of a healthy network design, the IP-addressing spaces of individual services and SPs should not overlap.

Nevertheless, this constraint cannot be enforced by an NP operating its network within a two-tier open-access model. The very separation of the services by means of VLANs prevents headaches for the NP

that might occur due to IP-addressing conflicts. Since each service is assigned its own unique VLAN for transport across the NP's domain, and since no routing takes place between the VLANs, even potentially overlapping IP-addressing spaces pose no problem: the services are distinguishable by their VLANs, and duplicated IP addresses from different VLANs never encounter each other.

Service provider's domain – Service-specific IP-address assignment

Each SP is responsible for the management of IP addresses within its domain: the IP addresses of the CPE are assigned by the SPs' DHCP servers. The SPs rely on (VLAN) "tunnels" through the NP's network to transport the DHCP communication only between the intended devices, i.e., within each SP's domain. A proper assignment of IP addresses to the CPE may be assisted using the DHCP option 60 (vendor ID) and option 43 (vendor-specific data).

The SPs manage IP addresses within their domains

2.4 Isolation of Customers' Flows

The VLANs on each individual BNT correspond to individual services that are used by the customer. Since different customers may use the same service of the same SP, their BNTs are members of the same service-specific VLAN. The same VLAN on several BNTs connected to the NP's Ethernet-bridged network might mean that the customers might be able to communicate directly across the NP's domain.

Yet they cannot. The "Private port" security feature on the MSANs enforces point-to-point operation of the VLAN "tunnels" and prevents direct communication between customers. Every service-specific VLAN "tunnel" only allows communications between a BNT and a BNG, but not between two BNTs directly. Naturally, the private-port feature also needs to be supported and enabled on the AGS.

Figure 4 illustrates a case of two customers that use the same two services from the same two SPs. (The management VLAN is not depicted for clarity reasons.)

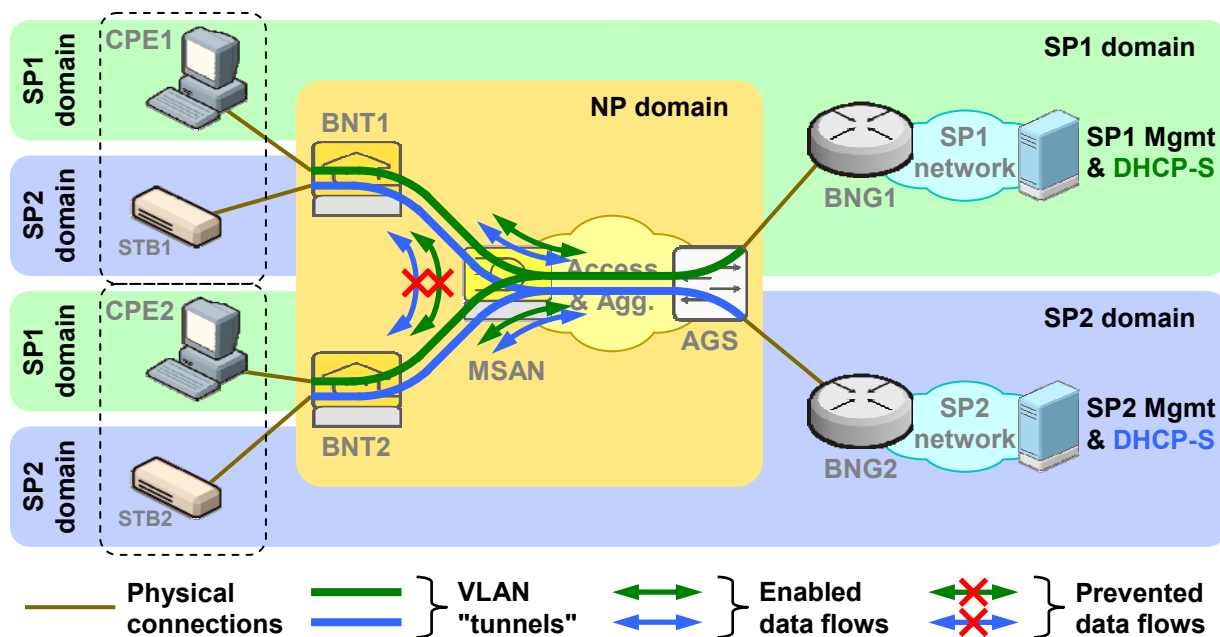


Figure 4: Isolation between customers using the same VLAN

Although the two customers' BNTs use the same two VLANs, communication paths are only established between the BNTs and the BNGs, while they are prevented between the two BNTs. This enforces proper service policing and billing, together with the protection of network resources.

2.5 VLAN-per-Service Architecture

The model uses the VLAN-per-service architecture for service delivery to customers. Using VLANs per service, all traffic flows are distinguishable and easily identifiable in the network; this identification is crucial for unambiguous service delivery, as well as for all quality-of-service and security processing.

Separating VLANs on a per-service basis means that the services are distinguishable solely based on the assigned VLAN IDs and no other means is needed. If the model did not use the VLAN-per-service architecture, the only way to distinguish the services would be to use an IP-address-based classification of all the packets. Not only would such an approach cause an extra processing load on the MSANs (with difficult-to-manage classification rules) – it would fail completely if the SPs used overlapping IP-address ranges. (Recall that within the two-tier open-access model, the NP cannot enforce the constraint of non-overlapping IP addresses upon the SPs.)

Proper identification of traffic flows is crucial for service delivery

Furthermore, the VLAN-per-service architecture allows the efficient delivery of video content to the customers, while optimizing the use of the NP's network resources. Iskratel's access products support the per-VLAN operation of IGMP snooping. Combining the VLAN-per-service architecture with the IGMP-snooping-per-VLAN functionality results in a per-service operation of the IGMP snooping, regardless of the SPs' IP-addressing schemes – even in the case of overlapping IP-address spaces, the IGMP snooping operates per service, efficiently protecting the network resources.

3 The Necessary Ingredients

3.1 Service-Selection Portal

Being given the possibility to choose and/or collect services from several service providers, the customers expect to be able to choose and select the services by themselves. The service-selection portal (SSP), an integral part of the open-access solution, represents a means for customers' service selection.

In effect, the SSP replaces a human operator or a customer-support desk to which a customer directs his or her requests regarding services. Automated service selection reduces the NP's operational costs and improves responsiveness and customer satisfaction.

The service-selection portal provides lower operational costs

The SSP is a part of the NP's management domain as a web-accessible application. The customer logs in to the SSP using a unique username and password. After being properly identified and authenticated, the customer may subscribe to new services, cancel existing services, or make changes to existing ones.

The SSP database

For proper operation, the SSP uses (and maintains) a database of customers and SPs and their services. This database is accessible from two sides: the customer's side and the NP's side. The customer's side is a web server, accessible via the internet using the SSP's public IP address. From this side, the customers manage their service subscriptions. The NP's side allows full management and control of the database, including the data that are invisible and inaccessible from the customer's side.

The SSP database contains relations between customers, SPs and services

The SSP database is composed of four parts:

- the service-description table (one entry per service per SP),
- the SP-description table (one entry per SP),
- the customer-description table (one entry per customer),
- the customer–service matrix (one entry per customer per service).

The former two (the service-description and the SP-description tables) are managed exclusively by the NP, while the latter two (the customer-description table and customer–service matrix) are managed by both the NP (full access) and the customers (partial access for service-subscription purposes only).

Using the SSP, customers review the available services (read parts of the service-description table), change their passwords (partially manage the customer-description table), and manage their subscriptions (partially manage the customer–service matrix).

Tables 1, 2, 3 and 4 show the contents of the SSP database in more detail. The symbols "■" denote read access from the customer's side; the symbols "◆" denote write access from the customer's side.

Service description	
Service ID	
Service-provider ID	
Service description	■
Service pricing	■
C-VLAN ID for this service	
S-VLAN ID for this SP (if any)	
DSCP and CoS values	
Required upstream/downstream bandwidth	■

Table 1: Service-description table

Customer description	
Customer ID	
User ID and password	◆
Customer description	■
Location ID (MSAN/slot/port IDs)	
Maximum available upstream/downstream bandwidth	■
BNT device type	
Number of CPE-facing ports on BNT	
BNT's MAC address	

Table 2: Customer-description table

SP description	
Service-provider ID	
Service-provider description	
List of SP's service IDs	
S-VLAN ID (if any)	
SP-facing port ID on the AGS	

Table 3: SP-description table

Customer–service matrix	
Customer ID	
Service ID	
CPE-facing port ID on the BNT, assigned for this service	◆
Time/date of service activation	■

Table 4: Customer–service matrix

The SSP's interfaces

To enable service changes, the SSP needs to interface with other components within both the NP's and the SPs' domains, and pass different configuration parameters to them. For example, when a customer subscribes to a new service, the SSP must forward the following service-related parameters to four affected components: the MSAN- and the BNT-management applications, the aggregation switch, and the SP's management systems.

- ➔ To the MSAN-management application:
 - C-VLAN and S-VLAN IDs
 - CoS value
 - BNT's location ID
 - BNT's MAC address
- ➔ To the aggregation switch:
 - C-VLAN and S-VLAN IDs
 - DSCP and CoS values
 - SP-facing port ID on the AGS
- ➔ To the BNT-management application:
 - C-VLAN ID
 - DSCP and CoS values
 - CPE-facing port ID on the BNT
- ➔ To the SPs' management system:
 - Service ID
 - Customer ID
 - Customer description

Depending on the agreement between the NP and an SP, other methods of NP–SP interworking are also possible; for example, the NP and an SP may agree on interfaces used for the notification of the SP's new services, of changes to existing services, etc.

3.2 Manageability of the Broadband-Network Termination

The model uses the VLAN-per-service architecture for service delivery to customers. This means that the VLANs on each broadband connection between the MSAN and a BNT directly correspond to services that are used by the customer. In addition, one VLAN on the broadband connection is used for the management of BNTs (Figure 3).

Individual VLANs map to physical ports of the BNT

Within the BNT, service VLANs map to physical CPE-facing Ethernet ports of the BNT. The service-to-port assignment is done by the customer via the SSP. This mapping is a part of the BNT's configuration. Figure 5 illustrates a BNT with eight CPE-facing ports, used for three types of services: internet access, video (two different services), and voice over IP (VoIP); four ports of the BNT remain unused. With the exception of the BNT-management VLAN, which is terminated on the BNT, the four service VLANs are mapped directly to the physical ports of the BNT.

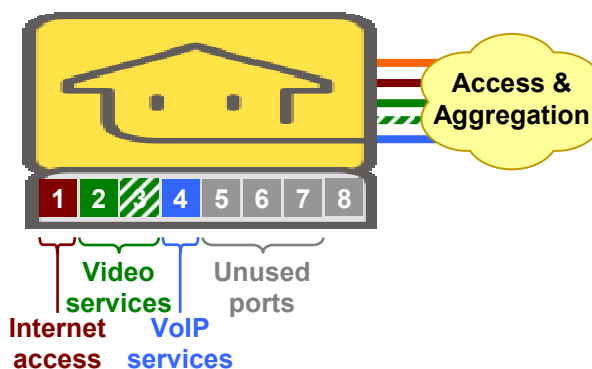


Figure 5: Service-to-port assignment on the BNT

In addition to the VLANs, other parameters may optionally be configured on the BNT, including service priorities (CoS) and rate limiting per service. The BNT can be managed via SNMP, CLI or hypertext-transfer protocol (HTTP). The preferred management method is the SNMP.

The BNT's configuration is stored on the BNT itself (runtime configuration) and on the NP's management platform. For the purpose of the auto-configuration of the BNT, it makes sense to bind the BNT's DHCP setup phase with an immediate download of the BNT's configuration. This setup phase is augmented with downloading of the BNT's firmware image (optional) and the active configuration parameters.

The necessary pre-configuration of the BNT

While the BNT is managed by the NP's management platform, any access to the management of the BNT by the customer must be prevented. The customer may not be given any administrative privileges on the BNT at all. If the customer could manage the BNT by himself or herself, he or she could (inadvertently or on purpose) misconfigure the BNT or even gain access to the NP's management domain.

In practice, this restriction requires that the BNT must be preconfigured by the NP before it is delivered to the customer.

- The BNT's default administrative password must be altered to one unknown to the customer.
- The DHCP client must necessarily be enabled on the BNT's broadband connection.
- The management VLAN must be configured on the BNT's broadband connection only.
- The access to the management VLAN must be prevented from the CPE-facing ports.

**The pre-configuration
of the BNT protects
the NP's network**

In addition, the customer needs to be able to access the SSP as soon as the BNT is delivered to him or her, plugged-in, and configured via the DHCP setup phase. For this purpose, the BNT's default configuration needs to include limited access to the internet via one (preferred) internet SP. Put technically, the BNT's default configuration parameters must also include a service VLAN to one internet SP, and this SP must have had this customer enabled on its management system and on the BNG. The default service VLAN gives the customer immediate access to the SSP: once logged in to the SSP, the customer may choose any services and/or change the default internet SP for another.

4 Putting It All Together

4.1 Bringing Services to Life

At the first power-on of the BNT and the activation of the broadband connection, as well as at any subsequent restart of the BNT, the BNT initiates a DHCP setup phase. This phase provides the BNT with its IP address, and – if DHCP option 43 (vendor-specific data) is used – with its latest firmware image and its configuration parameters. The management flow of an advanced DHCP setup for an automatic upgrade of the BNT's firmware image and configuration parameters is illustrated in Figure 6.

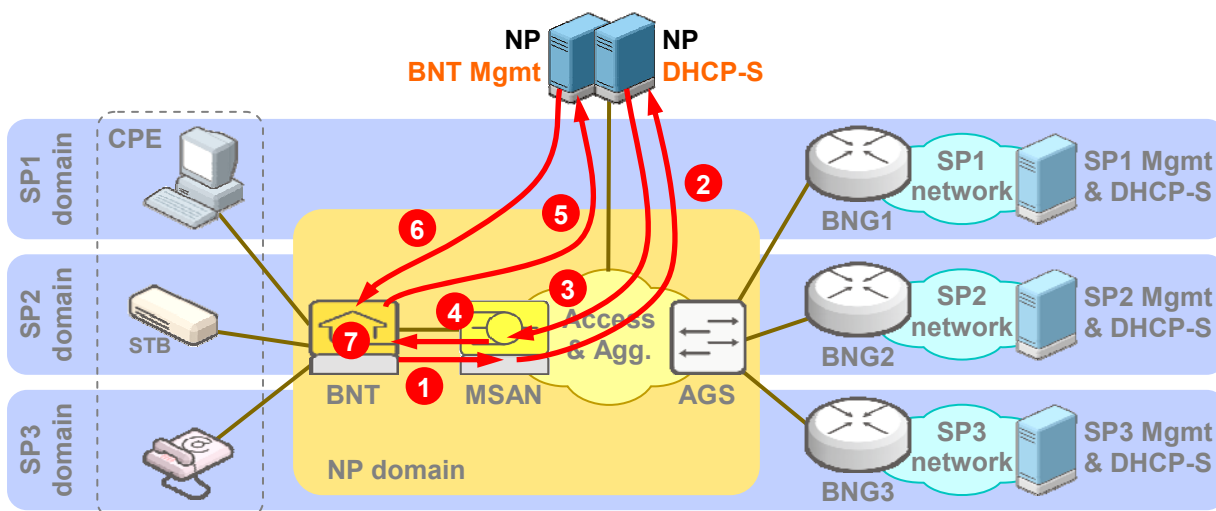


Figure 6: Automatic configuration of the BNT

The phases of the BNT's setup are the following:

- 1 The customer plugs in the BNT. The BNT sends an untagged DHCP-discovery message to obtain an IP address. The message may optionally include the DHCP option 60 (the BNT's vendor ID).
- 2 The DHCP-discovery message is intercepted by the MSAN. The MSAN inserts DHCP option 82 (line ID), tags the message with the BNT-management VLAN, and forwards it to the NP's DHCP server.
- 3 The NP's DHCP server uses the received DHCP options 60 (vendor ID) and 82 (line ID) to identify the customer and replies with a DHCP-offer message containing the assigned IP address; the reply may include the DHCP option 43 (vendor-specific data).
- 4 The MSAN strips off the DHCP option 82 (line ID) from the DHCP-offer message and forwards it to the BNT, leaving the DHCP option 43 (vendor-specific data) present.
- 5 The BNT sets the received IP address and uses the parameters from the DHCP option 43 (vendor-specific data) to request the proper firmware and configuration parameters from the NP's management platform via a trivial file-transfer protocol (TFTP) or a file-transfer protocol (FTP).
- 6 The NP's management platform downloads the proper firmware and configuration parameters to the BNT via TFTP or FTP.
- 7 The BNT applies its new firmware and new configuration parameters and reboots, if needed.

Auto-configuration of the BNT

For a further example, suppose that both the BNT and the NP's DHCP server support and understand the following sub-options of the DHCP option 43 (vendor-specific data):

- Download protocol (TFTP or FTP),
- IP address of the TFTP or FTP server,
- Username and password for download,
- Firmware image filename and its MD5 code,
- Configuration image filename and its MD5 code,
- Urgency (restart immediately after download or not).

The BNT's setup phase provides it with a complete configuration

To use these options, the NP's file server (which usually resides on the NP's management platform) must store the firmware image files and the configuration image files and recognize usernames and passwords for all the NP's BNTs and/or customers.

The NP's DHCP server recognizes the BNT's DHCP request based on the BNT's MAC address and/or the DHCP options 60 (vendor ID) and 82 (line ID). After receiving the DHCP reply with the DHCP option 43 (vendor-specific data), the BNT accesses the NP's file server via TFTP or FTP to download the firmware image and the configuration image. After the download, the BNT checks the downloaded files against their MD5 codes; if the check fails, the BNT retries the downloading, usually three times; if the checks fail again and again, the BNT will give up until the next DHCP message. If the check succeeds, and an immediate restart was required via the DHCP option 82, the BNT will restart to activate the new firmware and/or configuration immediately.

4.2 Selecting from among Services

When the customer's BNT is up and running and the customer is given access to the internet and to the SSP, the customer may access the SSP for service selection and customization. The management flow of an SSP-assisted service reconfiguration is illustrated in Figure 7.

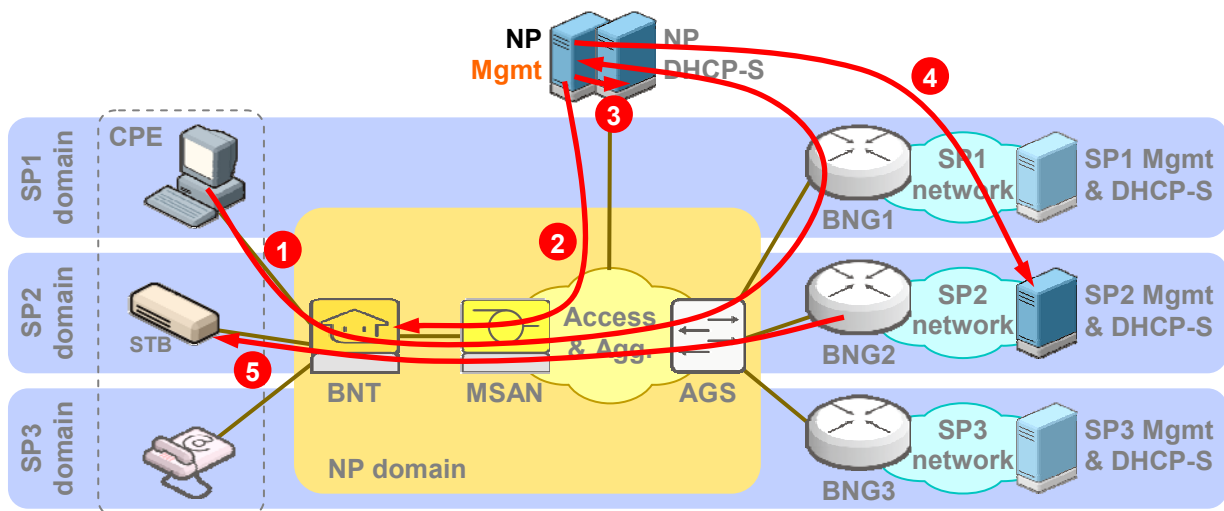


Figure 7: SSP-assisted service reconfiguration

The flow illustrates the case of a customer that already uses internet access from SP1, and also wants to subscribe to the video services of SP2. The steps in the management flow are as follows:

- ❶ The customer uses a personal computer to access the SSP via the internet (provided by SP1). He or she logs in to the SSP using the username and password. At the SSP, the customer subscribes to SP2's video service and chooses the port on the BNT to which the set-top box should be connected.
- ❷ The SSP notifies the MSAN-management application to enable the service on the MSAN, i.e., enable the service VLAN on the customer's port. The SSP also notifies the BNT-management application, which then reconfigures the customer's BNT in runtime: it enables the service VLAN on the BNT's broadband connection, binds it to the selected CPE-facing port, and sets service-specific parameters.
- ❸ The BNT-management application updates the BNT's active configuration on the DHCP and the file servers.
- ❹ The SSP notifies the SP2 of the new user of SP2's service. The SP2 enables access to the video services, administering its DHCP server and its BNG accordingly.
- ❺ When the customer receives SP2's STB, he or she is able to use SP2's video service immediately after having the STB plugged in.

The procedure sets a new VLAN "tunnel" between the designated port on the customer's BNT and the SP2's BNG. In this way, the STB, connected to the designated port, can communicate with the SP2's BNG directly; the communication is transparent to the NP's network. At each power-on of the STB, the STB will obtain its IP address from SP2's DHCP server, thus becoming ready for video service delivery. The whole process is transparent to the customer: having exploited the SSP's interface to subscribe to the service and having received the STB from the SP, the service is ready for the customer to start enjoying it immediately.

5 The Road Ahead

5.1 Service Integration and the Integrated Open-Access Model

In the two-tier model, any CPE device is owned by the SP that provides the service. This implies the replacement of the CPE when a customer chooses another SP for the same type of service. For example, if a customer switches video SP Alpha for video SP Omega, he or she needs to wait a day or two to get Omega's STB delivered; in the meantime, the customer is not able to receive Omega's video on the existing STB from Alpha.

In the two-tier model, again, a customer may collect services of the same type (e.g., video) from different SPs. However, the services cannot be integrated on a single CPE device (e.g., one STB) since the CPE is owned by individual SPs. Collecting services of the same type implies the multiplication of CPE devices (e.g., as many STBs as video SPs), leading to cabling mess, remote-control confusion and poor overall customer satisfaction.

Both of the above difficulties of the two-tier open-access model are overcome in the integrated open-access model [1].

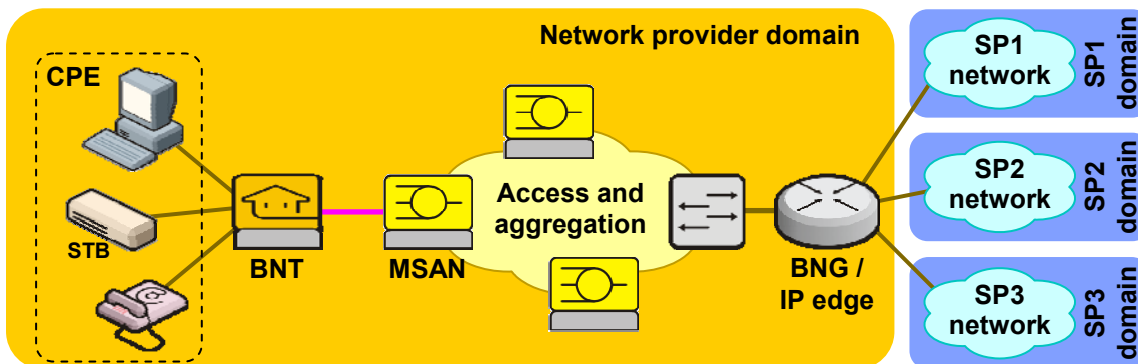


Figure 8: Integrated open-access model

In the integrated open-access model (Figure 8), both the BNT and CPE are owned by the NP. This way, customers can choose services from different SPs and even collect them without the need to have the CPE replaced or multiplied. Regardless of their choice of individual SPs, the customers keep their existing CPE. The specifics of the individual SPs are hidden from the customer by the NP.

The NP also provides its own BNG as a connection point for the SPs' specialized services. Therefore, it may also set the rules for connecting to its BNG. Specifically, the NP can impose service-related IP-addressing schemes to the SPs.

An NP, opting in for the integrated open-access model instead of the two-tier model, may count on better customer satisfaction and better control over network resources; on the other hand, the integrated model may require a bigger NT's capital expenditure.

5.2 Efficient and Secure Video Delivery

To facilitate an efficient multicast delivery of video and other multimedia content, while at the same time enforce the isolation of customers' flows, it is generally desirable to separate multicast and unicast video flows in the network. The STB normally employs both video-transport modes: unicast transport is used for video on demand (VoD), while video content like IP television (IPTV) uses multicast transport.

Efficient video delivery in a multi-provider environment

Following best practice in a healthy network design, Iskratel's MSAN offers its own patented functionality, the multi-provider multicast membership (MPMM). The MPMM provides the multicast–unicast separation as well as proper multicast–multicast separation of video flows in a multi-provider environment.

**MPMM: A necessity
in a multi-provider
environment**

For example, if a customer uses a single STB to receive IPTV and VoD services from the same SP, a single video VLAN is used for both IPTV and VoD on the broadband connection. The MPMM on the MSAN, however, separates the two flows into two distinct

VLANs in upstream: one for IPTV and one for VoD. In downstream, the MPMM combines the two VLANs into a single video VLAN, delivered to the customer's STB.

Easy service collecting

In the two-tier and the integrated open-access models [1], the customers may receive video services from different SPs on a single STB. In this case, the MPMM proves itself invaluable: in upstream, it separates the video flows into distinct VLANs to different SPs; in downstream, the MPMM combines several video VLANs into a single video VLAN, delivered to the customer's STB.

Finally, it should come as no surprise that the MPMM is even able to operate on untagged data flows, extract video streams and separate them into distinct VLANs. The only precondition for such operation is non-overlapping IP-addressing spaces, assigned to the services.

**MPMM: Invaluable
when customers
collect services**

5.3 Extending the Service Provider's Reach

Before the transition to the traditional wholesale model that introduced a formal separation of network operators and service providers, the operators used their home gateways (HGWs) both to terminate the broadband connection and to terminate the higher service-related layers (for example, a HGW may have integrated a VoIP-to-POTS adapter).

The transition to the wholesale model forced the operators to adapt their businesses and begin operating as either an NP or an SP. With the transition to the wholesale model, and even more so with the transition to the open-access model, the SPs' HGWs lost their role of the demarcation point (terminating the broadband connection) and this role was taken over by the NP's BNT.

Nevertheless, the SPs are interested in keeping their existing business model even when they deliver their services over another NP's network. This means that the SPs wish to use their existing HGWs even when they do not need to terminate the broadband connection. In the open-access model, these devices become a part of the CPE.

To operate as the service-layer termination points, the HGWs need to be managed: beside the service-related VLANs, the HGWs require another VLAN for their management (which is performed by the SP). Figure 9 illustrates the case of a customer that uses three services from two SPs.

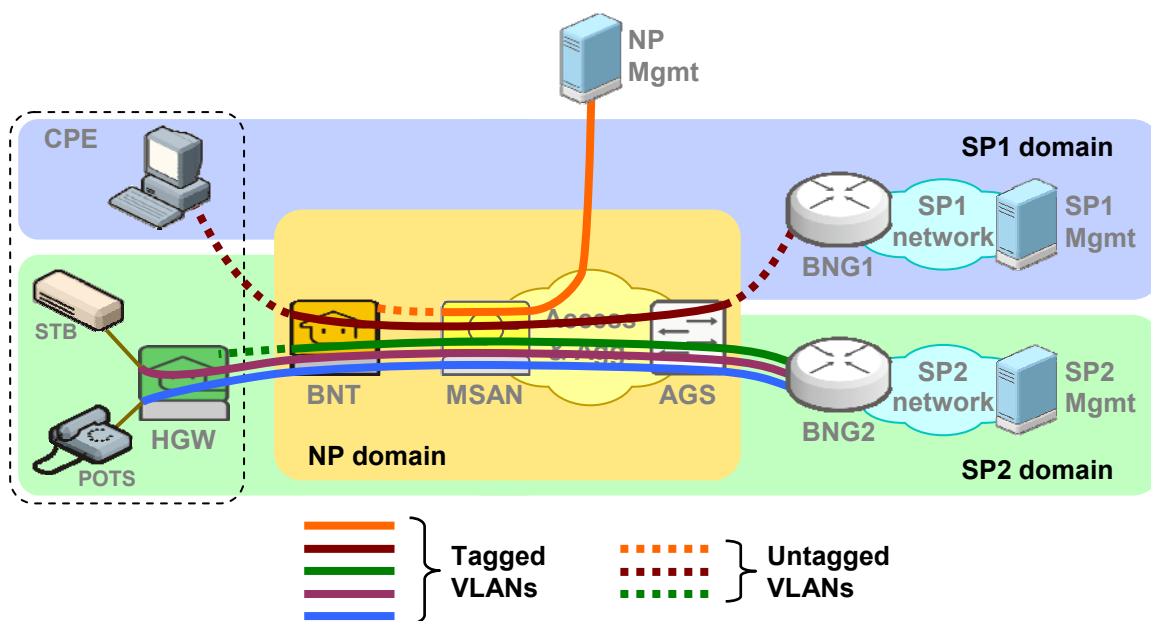


Figure 9: SP's home gateway as a part of the CPE

On the customer's BNT, two customer-facing ports are occupied.

- The first port is used for SP1's internet-access service. A personal computer is connected directly to this port. Through the NP's network, a single dedicated VLAN provides a path for the service.
- The second port is used for SP2's video and voice services. A home gateway provided by the SP2 is connected to this port; the SP2's set-top box and a POTS phone connect to the HGW. Through the NP's network, two dedicated VLANs transport the two services, while the third VLAN is used for the management of the HGW. The second port on the BNT carries tagged and untagged Ethernet frames to support the service-related VLANs as well as the HGW-management VLAN.

The customer-facing ports on the BNT operate in mixed mode: some physical ports are mapped directly to the service VLANs (one service per port), while other ports convey multiple service VLANs. The mode of operation of each individual physical port on the BNT is dictated by the business model used by the SP that provides the service (or services) to that port. This requires the service-selection portal to support the assignment of individual services, as well as the assignment of the SPs' service packs to the individual ports on the BNT.

5.4 Transparent Management – Gemini is the Future

Using a general or third-party BNT requires the BNT to be manageable via its assigned IP address. As shown, this implies the use of the BNT-management application and the DHCP server for the assignment of the BNT's IP address. The NP's management platform can be simplified if the BNT is chosen to be manageable via a layer-two (Ethernet) protocol, without the need for a unique IP address on each BNT.

Iskratel's new BNT, the Gemini, allows its management via an extension of standard Ethernet operations, administration and maintenance (Ethernet OAM) protocol, without the need for an IP address (Figure 10).

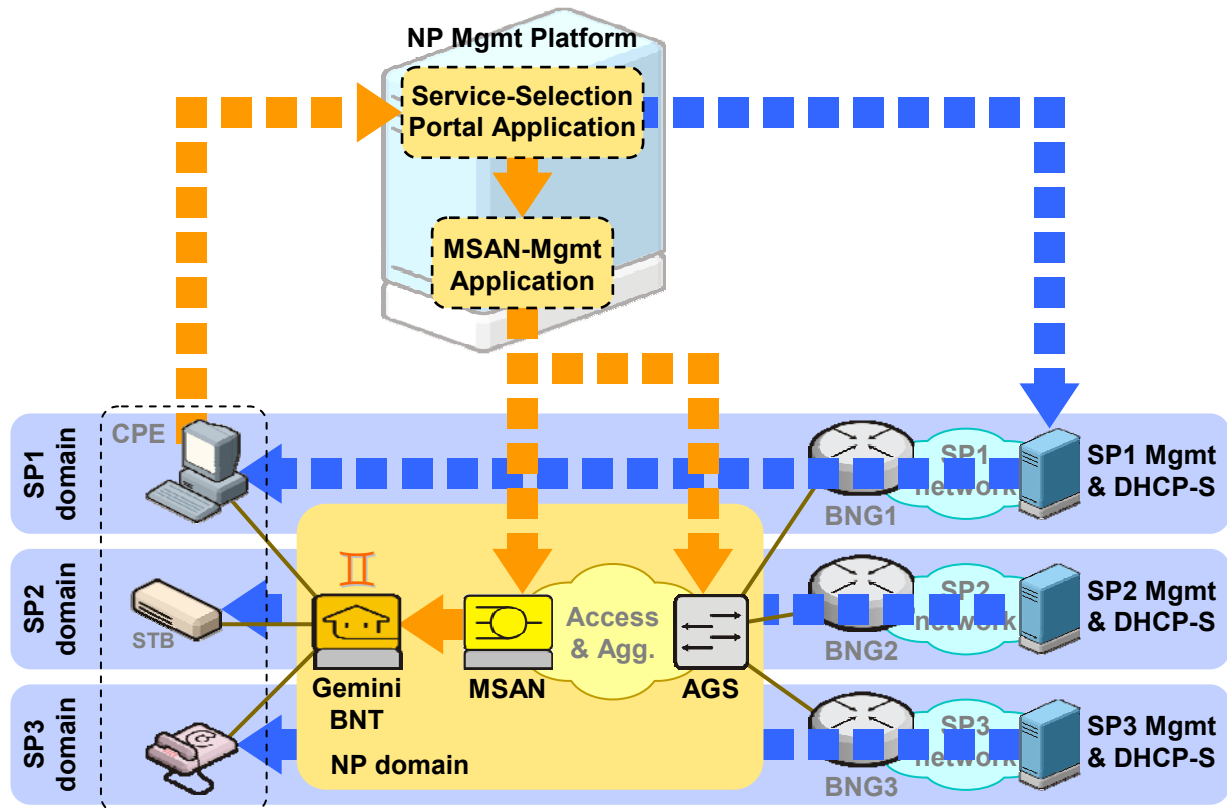


Figure 10: Management domains and flows with the Gemini BNT

The Gemini BNT is managed directly from the MSAN. Gemini's management is completely transparent to the NP's management platform.

The Gemini BNT keeps all the features of an IP-equipped BNT. At the same time, however, its use simplifies the management principles and decreases the cost of operating the network.

6 Final Thoughts

The implementation of the two-tier open broadband access using Iskratel's access products is a straightforward, headache-free process. Applying network-design concepts that allow a clear division between management and awareness domains allows network and service providers alike to optimize their operation and management processes. This optimization results in an efficient delivery of services to the customers and in a user-friendly means of service selection and customization, improving customer satisfaction and making the business success of service providers and network providers possible.

7 Abbreviations

AGS	Aggregation Switch
BNG	Broadband Network Gateway
BNT	Broadband Network Termination
C-VLAN	Customer VLAN
CLI	Command-Line Interface
CoS	Class of Service
CPE	Customer-Premises Equipment
DHCP	Dynamic Host-Configuration Protocol
DHCP-S	DHCP Server
DSCP	Differentiated Services Code-Point
FTP	File-Transfer Protocol
HGW	Home Gateway
HTTP	Hypertext-Transfer Protocol
ID	Identity
IGMP	Internet Group-Management Protocol
IP	Internet Protocol
IPTV	IP television
MAC	Medium-Access Control
MD5	Message-Digest Algorithm 5
Mgmt	Management
MPMM	Multi-provider multicast membership
MSAN	Multi-Service Access Node
NP	Network Provider
OAM	Operations, Administration and Maintenance
POTS	Plain Old Telephone Service
S-VLAN	Service VLAN
SNMP	Simple Network-Management Protocol
SP	Service Provider
SSP	Service-Selection Portal
STB	Set-Top Box
TFTP	Trivial File-Transfer Protocol
VLAN	Virtual Local-Area Network
VoD	Video on demand
VoIP	Voice over IP

8 References

- [1] T. Bogataj, *Towards a Customer-Friendly Open Broadband Access*, Technology whitepaper (code MAD075300-GKE-010), Iskratel, February 2009

ISKRATEL

Iskratel Ltd., Kranj

Ljubljanska cesta 24a, SI 4000 Kranj, Slovenia
phone +386 4 207 2000, fax +386 4 207 2712

info@iskratel.si
www.iskratel.com

ISKRATELGroup

Iskratel Electronics, Ljubljanska cesta 24a, SI 4000 Kranj, Slovenia, phone +386 4 207 3496, fax +386 4 207 2991, e-mail: info-ite@iskratel.si, www.iskratel-electronics.si
Iskrateling, Ljubljanska cesta 24a, SI 4000 Kranj, Slovenia, phone +386 4 207 6276, fax +386 4 207 6277, e-mail: info@iskrateling.si, www.iskrateling.com
Monis, Oktyabrskoy revolucii str. 99, UA – 61157 Harkov, Ukraine, phone +380 577 15 80 00, fax +380 577 15 80 16, e-mail: monis@monis.com.ua, www.monis.com.ua
Iskrauraltel, Komvuzovskaya str. 9a, 620137 Yekaterinburg, Russian Federation, phone +7 343 210 69 51, fax +7 343 341 52 40, e-mail: iut@iskrauraltel.ru, www.iskrauraltel.ru
Iskrabel, Harkovskaya str. 1/601, BY - 220073 Minsk, Belarus, phone +375 17 213 03 36, fax +375 17 251 74 59, e-mail: pihtin@iskrabel.by
Iskracom, Naurizbay batyra 17, office 213, 050004 Almaty, Kazakhstan, phone +7 327 2917 166, fax +7 327 2917 166, e-mail: a.nikonov@mail.ru
ITS Iskratel Skopje, Kej 13 Noemvri, Kula 4, 1000 Skopje, Macedonia, phone +389 2 323 53 00, fax +389 2 323 53 99, e-mail: info@its-sk.com.mk, www.its-sk.com.mk